このリリースについて

Mar 14, 2016

Citrix Receiver for Windowsを使用して、ユーザーはXenAppサーバーやXenDesktopサーバーで公開されている仮想デスクトップやアプリケーションに安全にアクセスできます。

このリリースでの新機能

HDX RealTime Media Engine (RTME)の既知の問題

Citrix Receiver for Windowsのこのリリースでは、RTMEを統合してダウンロードとインストールが一度で済むパッケージにすることにより、インストール作業がより簡単になりました。 これまでは、ユーザーがCitrix Receiverをインストールしてから、RTME機能をReceiverに統合するために、MSIインストールパッケージを別途起動する必要がありました。

これによって、ユーザーの手間が省かれ、企業によってはHDX RealTime Optimization Packの採用が加速しました。以前は、BYODユーザー(とリモートワーカー)は、最初にCitrix Receiverをインストールし、次にCitrixのダウンロードページに戻って、HDX RTMEのためのインストーラーを別途起動する必要があったためです。 単一のインストーラーでは、最新のCitrix Receiver for WindowsとHDX RTMEインストーラーが結合されています。

HDX RTMEが統合され、1つの実行可能ファイルになった最新のCitrix Receiverインストーラーについて詳しくは、「インストール」を参照してください。

セッション画面グループポリシーを使用した透過性レベルの設定

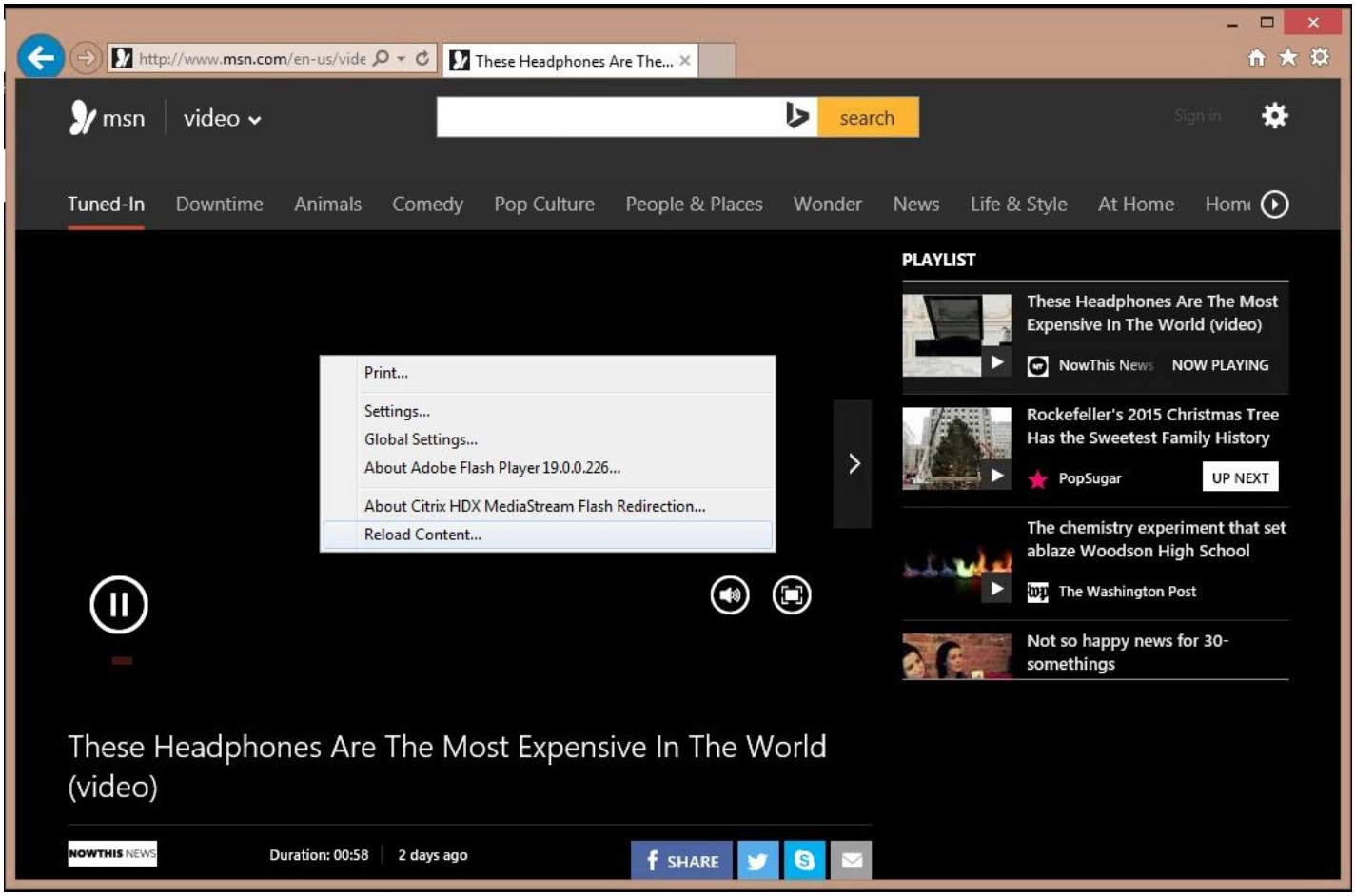
このリリースではセッション画面の保持グループポリシーを強化しています。 セッション画面の保持グループポリシーを構成すると、セッション画面の保持再接続期間の間に公開アプリケーション（またはデスクトップ）に適用される透過性レベルを設定できるようになりました。 詳しくは、「**グループポリシーオブジェクトテンプレートによるReceiverの構成**」で「セッション画面の保持およびグループポリシー」を参照してください。

サーバー側レンダリングへの手動フォールバック

このリリースのCitrix Receiverでは、クライアント上でのサーバー側レンダリングへの手動フォールバックが導入されています。 Flashコンテンツを表示する場合に状況によっては、クライアントの画面が黒くなり、Flashビデオを表示できないことがあります。 ほとんどの場合、Flashをクライアント上でレンダリングできないと、サーバー側レンダリングに自動的にフォールバックします。 ただし、場合によっては、クライアント側レンダリングに失敗してフォールバックもできないことがあります。

このような問題を解決するため、Citrix Receiver for Windowsでは、ユーザーが手動で画面を更新してFlashコンテンツのサーバー側レンダリングを実行するオプションが提供されています。 手動でフォールバックするには、カーソルを黒くなったFlashウィンドウに置いて右クリックし、［Reload content］を選択します。 次の図はこの機能を示します。

> ### 注意
>
> 管理者により設定されたビデオ防止ポリシーがクライアントに適用されます。詳しくは、「マルチメディアのポリシー設定」および「Flashリダイレクトのポリシー設定」を参照してください。



SSL SDKライブラリのアップグレードによるNIST SP800-52のサポート

Citrix ReceiverはアップグレードされたSSL SDKライブラリを提供し、NIST SP800-52をサポートするようになりました。 This functionallity allows Receiver to support the NIST SP800-52 compliance mode for TLS connections. 詳しくは、「クライアントのアクセス許可を設定するには」の「NIST SP800-52準拠モードの有効化」を参照してください。 セッション画面の保持について詳しくは、「**グループポリシーオブジェクトテンプレートによるReceiverの構成**」の「セッション画面の保持およびグループポリシー」参照してください。

アップグレード処理の改善

このリリースのCitrix Receiver for Windowsでは、既存のクライアント設定をそのまま維持する更新されたインストーラーが提供され、Citrix Receiverの以前のバージョンから更新した場合におけるユーザーエクスペリエンスが向上します。 さらに、更新されたインストーラーは以前にインストールされたバージョンからシームレスにアップグレードします。

クライアントの自動再接続とセッション画面の保持の改善

これらの改善により、CloudBridgeとNetScaler Gatewayの相互運用性がより向上しています。 セッションは、接続パスには関係なく、クライアントの自動再接続とセッション画面の保持を使って再接続できます。 このリリースに特定の拡張は以下の通りです。

- 機能強化された接続メッセージによりユーザーに接続状況が示され、またいつ接続が失われ、何するのかが通知されます。
- カウントダウンタイマー（分/秒単位）により、セッションがタイムアウトするまでの時間が示されるようになりました。セッションは、カウントダウンタイマーの有効期限が切れると中断されます。 デフォルトでは、タイムアウト値は2分に設定されています。 デフォルト値は、TransportReconnectMaxRetrySeconds ICAファイル設定で変更できます。

HDXパフォーマンスの向上

Citrix Receiverは更新され、クライアント側のハードウェアアクセラレーションが強化されました。 この機能により、ハードウェアアクセラレーションを有効にしてクライアント上でのHDX 3D Proのパフォーマンスが向上します。 この機能の構成について詳しくは、ユーザーエクスペリエンスアーティクルの「ハードウェアのデコード」を参照してください。

認証プラットフォームへの拡張

Citrix Receiver for Windowsは、特定の暗号化アルゴリズム、モード、キーサイズ、およびSecureICAが有効かどうかについての検証を含む、特定のTLSバージョンを使用しているサーバーにクライアントがどのように接続するのかを検証する方法を改善する機能が統合されています。 この機能を使って、アクティブなセッションでクライアントが使用する現在の認証証明書を表示することもできます。 詳しくは、暗号の使用について議論しているXenApp - XenDesktop articleを参照してください。

改善された起動ダイアログメッセージ

このバージョンでは、システム関連の変更および更新についてユーザーに通知する場合に、Citrix Receiver for Windowsが起動ダイアログを使用する方法が改善されています。 セッションの起動時に、以前のような大量のシステムレベルの通知が表示されるのではなく、簡素な通知が表示されるようになりました。

強化された診断情報の収集

このリリースでは改善された診断ツールを統合しています。このツールは、システム情報を素早く収集するために使用することができ、また簡単に転送したりCISのようなサービスにアップロードしたりすることが可能な単一の圧縮パッケージを作成して情報を配信できます。

このリリースで解決された問題について

重要：XenAppまたはXenDesktop 7.6を使用している場合は、CTX142037、CTX142094、およびCTX142095から入手できるVDA Hotfixのインストールを検討してください。 このHotfixにより、セッションに再接続した後のオーディオの問題や、特定の条件下で発生するグラフィックの表示レスポンス、イメージ品質、および画面表示の問題が解決されます。

Citrix Receiver for Windows 4.4で解決された問題

Jan 27, 2017

Receiver for Windows 4.4 CU3（4.4.3000）

Citrix Receiver for Windows 4.4 CU2（4.4.2000）との比較

Receiver for Windows 4.4 CU3（4.4.3000）には、Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100、4.1.200、4.2、4.2.100、4.3、4.3.100、4.4、4.4 CU1（4.4.1000）、4.4 CU2（4.4.2000）に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

ローカルアプリケーションアクセス

- ローカルアプリケーションアクセスを使用すると、特定のソフトフォンアプリケーションやChromeが正しく表示されないことがあります。

  [#LC4327]

- ローカルアプリケーションアクセス（LAA）デスクトップから切断し、全画面モードの非LAAデスクトップに接続すると、クライアント側のタスクバーが全画面モードの非LAAデスクトップの上に表示されることがあります。

  [#LC5966]

- セッション画面を全画面からウィンドウモードに切り替えると、次のメッセージを表示するダイアログボックスが開きません。
  「セッションがウィンドウモードです。 一部のLAA機能は、このモードで機能しない可能性があります。」
  ウィンドウモードでアプリを起動すると、次のメッセージを表示するダイアログボックスが開きません。
  「アプリの起動エラー。 セッションがウィンドウモードです。 このモードは、LAAアプリの起動を禁止します。 起動を続行するには、全画面モードに切り替えてください。」

  [#LC6291]

- ローカルアプリケーションアクセスが有効な場合、デスクトップセッションは強制的に全画面モードで起動します。

  [#LC6294]

メモリ、CPUの最適化

- SelfServicePlugin.exeプロセスによってメモリの消費量が多くなることがあります。

[#LC4509]

セッション/接続

- 移動ユーザープロファイルを使用してログオンし、公開アプリケーションを開くと、ファイルの種類の関連付けが機能しないことがあります。

  [#LC5184]

- SpeechMikeを別の音声認識アプリケーションとともに使用して口述すると、SpeechMikeが停止することがあります。

  [#LC5632]

- サイレントスイッチをオンにしてCleanUp.exeプロセスを使用すると、Citrix Receiverが適切に再読み込みされません。

  [#LC6039]

- HDX Engineが、予期せず終了する場合があります。

  [#LC6047]

- NetScaler Gateway 11でWyseシンクライアントからデスクトップを起動しようとすると、次のエラーメッセージが表示されることがあります。

  「クライアントからサーバーへの認証で問題が発生しました（Your client has experienced a problem with authentication to the server）」

  [#LC6145]

- セッション画面を継続的に移動すると、セッションが終了するかフリーズすることがあります。

  [#LC6403]

スマートカード

- Citrix Receiver for Windows 4.4をインストールすると、XenApp 6.5の公開アプリケーションがスマートカードにトランザクション要求を送り、アクティブではないトランザクションを終了することがあります。 Citrix Receiver for Windowsがこの要求に誤って応答することがあり、XenAppサーバーが応答をいつまでも、または設定されたトランザクションタイムアウト値に達するまで待機します。

  [#LC5772]

ユーザーエクスペリエンス

- この修正により、クライアントオーディオのリアルタイムモードを使用して短時間再生されるサウンドのサポートが強化されます。 この修正は、中音質のみに適用されます。

  [#LC4941]

- Windows 8.1およびWindows Server 2012 R2を使用すると、ファイルの種類の関連付けがファイルの種類を正しいアイコンおよびアプリケーションに関連付けないことがあります。 この修正では、［SelfService］に導入された2つのグループポリシーがあります。
  1. デフォルトFTAを有効にします - FTAのデフォルトの動作を有効または無効にする
  2. FTAを有効にします - FTA機能を有効または無効にする

ファイルの種類の関連付けで適切なアイコンを取得するには、グループポリシー［デフォルトFTAを有効にします］を無効にします。

[#LC5485]

- ファイルの種類の関連付け（FTA）のアイコンは、次の場合にデフォルトのCitrix Receiver for Windows FTAアイコンのように動作することがあります。公開デスクトップにログオンするとき、またはCitrix Receiver for Windowsの構成をリセットする場合。

  [#LC5730]

- Surface Pro 4およびHP EliteのWebカメラがセッションにリダイレクトしないことがあります。 注：Webカメラが画面解像度をサポートしない場合、Webカメラのリダイレクトも失敗することがあります。

  この問題を解決するには、次のレジストリキーを使用します。
  HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
  値の名前：DefaultWidth
  種類：Dword
  値：<Webカメラがサポートする解像度> 例（Surface Pro 4）：1920

  HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
  値の名前：DefaultHeight
  種類：Dword
  値：<Webカメラがサポートする解像度> 例（Surface Pro 4）：1080

  [#LC5750]

- クライアント名で割り当てられたデスクトップが［SelfService］画面で正しく表示されません。 この問題は、StoreFrontの統合エクスペリエンスを使用すると発生します。

  [#LC5773]

Receiver for Windows 4.4 CU2（4.4.2000）

Citrix Receiver for Windows 4.4 CU1（4.4.1000）との比較

Receiver for Windows 4.4 CU2（4.4.2000）には、Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100、4.1.200、4.2、4.2.100、4.3、4.3.100、4.4および4.4 CU1（4.4.1000）に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

HDX MediaStream Flashリダイレクト	ユーザーエクスペリエンス
キーボード	ユーザーインターフェイス
ローカルアプリケーションアクセス	Web Interface
セッション/接続	その他
システムの例外	

HDX MediaStream Flashリダイレクト

- SOLFileHookが有効な場合、ProofHQ.comのFlashコンテンツが正しく再生されません。

  [#LC4866]

- Adobe Flash Playerのバージョン22または18.0.0.360を使用して、FlashコンテンツのWebサイトを表示すると、WebサイトのURLがDynamic Blacklistに追加され、ユーザーデバイスではなくサーバーでレンダリングされます。

  [#LC5626]

キーボード

- ユーザーデバイスでキーボードショートカットポリシーが有効になっており、wfica32プロセスが実行されている場合、［リモートデスクトップ接続］で接続すると「ヒント：全画面モードを終了している」ダイアログボックスが開くことがあります。 キーボードおよびマウスからダイアログボックスに入力できないことがあります。

  [#LC4445]

- Microsoft Surface Proデバイスで外部USBキーボードまたはワイヤレスキーボードを使用して文字を入力するたびに、Citrix Receiver for Windowsセッションでローカルのスクリーンキーボードが表示されることがあります。

  [#LC5093]

ローカルアプリケーションアクセス

- ローカルアプリケーションアクセスを有効にすると、全画面モードまたはウインドウモードのリモートセッションでアプリケーションを起動した場合、アプリケーションアイコンがVDAセッションのタスクバーで表示されないことがあります。 エンドポイントで、1つではなく複数のアプリケーションアイコンがタスクバーに表示されることがあります。

  [#LC4217]

- ローカルアプリケーションアクセスを有効にして公開デスクトップセッションを起動すると、Desktop Viewerツールバーが表示されなくなることがあります。

  [#LC5064]

- ローカルアプリケーションアクセスを有効にしたVDAに接続した場合、エンドポイントデバイスのVDAセッションでALT+TABを押すと、タスクスイッチャーが断続的に表示されます。

  [#LC5084]

- ローカルアプリケーションアクセスが有効なデスクトップで、ウインドウモードから全画面モードに変更すると、正しくレンダリングされないことがあります。

  [#LC5091]

- ローカルアプリケーションアクセスを有効にしたVDAからの接続を切断すると、タスクバーが［自動非表示］モードのままになることがあります。

  [#LC5183]

セッション/接続

- NetScalerのクライアント証明書認証を［Optional］に設定して、証明書の要求をキャンセルしようとすると、不明のクライアントエラー1110で公開アプリケーションの起動に失敗することがあります。

  [#LC4169]

- ユーザーの簡易切り替え機能がある複数画面セッションで、クライアントマシンに再接続後、1つの画面でのみセッションが表示されることがあります。

  [#LC4382]

- ユーザーデバイス1からシームレスアプリケーションを起動し、RDPでユーザーデバイス2から1に接続する場合、起動されたシームレスアプリケーションが全画面モードになり、ユーザーデバイス1のタスクバーを隠すことがあります。 最小化し、アプリケーションウインドウを復元した後でも、問題は解決しません。

  [#LC4682]

- NetScaler Gatewayで接続されたセッションが、大幅に帯域幅を消費し、応答しなくなることがあります。

  [#LC4710]

- Cisco WAASのような特定のサードパーティ製ソフトウェアを使用すると、Citrix Receiver for Windowsの接続が切断されることがあります。

  [#LC4805]

- この修正は、基本コンポーネント内のメモリ問題に対応しています。

  [#LC4903]

- Citrix Receiver for Windows 4.4にアップグレード後、最初のログオンでアプリケーションの起動に断続的に失敗し、Citrix Receiver for Windowsの再起動が必要になることがあります。 次のエラーメッセージが表示されます：

  「アプリケーションを開始できません。 ヘルプデスクに連絡してください。」

  [#LC4975]

- StoreFrontからCitrix Receiverでアプリにアクセスしようとすると、ユーザーデバイスによっては失敗することがあります。ストアの追加に成功した後、列挙処理中に以下のメッセージが表示されることがあります。

  「サーバーに接続できません。
  ネットワークを確認して
  再試行してください。」

  [#LC5039]

- Single Sign-onプロセス（SSONSvr.exe）が予期せず終了するか、資格情報がログオン画面に自動的に渡されず、資格情報の手動入力を要求するメッセージが表示されることがあります。

  [#LC5123]

- Citrix Receiverは、Internet Explorerでプロキシバイパス一覧を無視します。

  [#LC5131]

- Citrix Receiver for Windowsをインストールして、レジストリエントリまたはGroup Policy Object（GPO）経由でストアを

構成すると、仮想マシン（VM）の再起動後の最初のログオンで、アプリケーションが列挙できないことがあります。

[#LC5198]

- Microsoft Internet Explorerで［設定を自動的に検出する］オプションを有効にすると、Citrix Receiverでアプリケーションの列挙が遅くなることがあります。

  [#LC5224]

- Framehawkを有効にすると、XenDesktop 7.8のVDAセッションで、マウスのスクロールボタンによる操作が実行されないことがあります。 XenDesktop 7.9で、対応するVDA側の修復を利用できます。

  [#LC5302]

- ［スタート］メニューからアイコンをクリックして、アプリケーションを起動しようとすると、既にログオンしている場合でも断続的に失敗することがあります。

  [#LC5306]

- Androidデバイスで、Citrix Receiver for Windows 4.4を使用する場合、最初のホップセッションで、wfica32.exeプロセスが終了することがあります。 ダブルホップ環境のユーザーセッションで公開アプリケーションを起動しようとすると、問題が発生します。

  [#LC5391]

- タッチおよびドラッグジェスチャ中、シームレスEPICアプリケーションを使用すると、マウスボタンがダウン状態のままになることがあります。 シームレスEPICアプリケーションのウインドウ外でタッチ入力を解放すると、セッションが応答しなくなることがあります。

  [#LC5644]

システムの例外

- 以下のメッセージが表示され、Citrix Receiver for Windowsが予期せず終了することがあります。

  「Citrix HDX Engineが動作を停止しました」

  [#LC4100]

- Windows Media Playerで.aviファイルを繰り返し再生すると、wfica32.exeプロセスがデッドロックになり、予期せず終了することがあります。

  [#LC4587]

- プロキシ経由で公開アプリケーションを起動すると、以下のエラーメッセージが表示され、Citrix Receiver for Windowsが予期せず終了することがあります。

  「Citrix HDX Engineが動作を停止しました」

  [#LC5149]

- Windows VistaでCitrix Receiver for Windows 4.4をインストール後、アカウントを追加しようとすると、Citrix Authentication Manager（AuthMgrSvr.exe）が予期せず終了することがあります。

  [#LC5242]

ユーザーエクスペリエンス

- ローカルアプリケーションアクセスが有効になると、セッション画面が最大化された状態から復元され、Desktop Viewerウインドウの外に配置されることがあります。

  [#LC2930]

- タッチおよびドラッグジェスチャ中、Citrix Receiver for Windowsからのタッチ入力によって、意図しないマウスイベントをサーバーに送信することがあります。 これにより、シームレスEPICアプリケーションが応答しなくなることがあります。

  [#LC5459]

ユーザーインターフェイス

- StoreFrontの統合エクスペリエンスでサブスクリプションが解除されたコンテンツを開こうとすると、以下のエラーメッセージが表示され、失敗することがあります。

  「必要なソフトウェアがインストールされてないため、アプリケーションを起動できません。」

  [#LC4308]

- 英語以外のオペレーティングシステムでは、Receiver for Windowsで表示されるプロトコルエラー1030のテキストが文字化けします。

  [#LC4687]

- ローカルアプリケーションアクセスを有効にしてスキンモードでVLC Media Playerを使用すると、エンドポイントがタスクバーのショートカットを1つではなく複数表示することがあります。

  [#LC4744]

- シームレスモードのMicrosoft Internet Explorerで公開されたインスタンスで、GoToMeeting URLを使用してタスクバーを起動すると、GoToMeetingアイコンがタスクバーに表示されません。

  [#LC4810]

- FastConnect APIユーザー間で切り替えると、以下のエラーメッセージが表示されます。

  「現在、アプリケーションを使用できません。 しばらく待ってから再試行してください。」

  また、FastConnect APIを使用してログオンすると、前のユーザーアプリケーションショートカットがデスクトップから削除されます。

  [#LC5602]

Web Interface

- ユーザーデバイスで以前のバージョンのCitrix Receiver for Windowsがインストールされていると、Web InterfaceにCitrix Receiverインストールページが表示されません。

  [#LC4242]

その他

- wfica32.exeプロセスによりCPUが100%使用されることがあります。

  [#LC4520]

- 次のようなコマンド「SelfService.exe command, -init –createprovider」を使用してストアを作成すると、関連するレジストリキーが正しく作成されます。例：C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\SelfService.exe -init -createprovider store https://<StoreFrontURL>/Citrix/store/discovery。 通知領域でReceiverアイコンをクリックして、SelfServiceユーザーインターフェイスにアクセスすると、ストアはレジストリから削除され、［アカウントの追加］ダイアログボックスが開くことがあります。

  [#LC5096]

- wfica32.exeプロセスによりCPUが100%使用されることがあります。

  [#LC5189]

- 初回の起動、および「Do not ask me again for this virtual desktop（仮想デスクトップを確認しない）」オプションを選択した後の起動でも、Client Selective Trust（CST）設定が維持されず、「HDXファイルアクセス」というメッセージが表示されることがあります。 レジストリキー「HKEY_Current_User\Software\Citrix\Ica Client\Client Selective Trust」で同じVDAに新しいレジストリが作成されると、オプションを選択した後でもこの問題が発生します。

  [#LC5598]

- NetScalerでTLSv1.2を構成すると、外部Windows 7ユーザーデバイスが StoreFrontアカウントを追加できないことがあります。 次のエラーメッセージが表示されます。

  「認証サービスにアクセスできませんでした。」

  [#LC5737]

Receiver for Windows 4.4 CU1（4.4.1000）

Citrix Receiver for Windows 4.4との比較

Receiver for Windows 4.4 CU1（4.4.1000）には、Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100、4.1.200、4.2、4.2.100、4.3、4.3.100および4.4に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

クライアントデバイスの問題	シームレスウィンドウ
HDX MediaStream	セッション/接続
インストール、アンインストール、アップグレード	システムの例外
キーボード	ユーザーエクスペリエンス
ローカルアプリケーションアクセス	ユーザーインターフェイス
印刷	

クライアントデバイスの問題

- USB 3.0で接続したCitrix Receiver for Windows 4.3デバイス（キーボード、マウスデバイスなど）を使用しているときに、重作が停止し「DRIVER_POWER_STATE_FAILURE (0x9f)」というエラーが表示されることがあります。

  [#LC4542]

- Surface Proタイプカバーおよびタッチカバーデバイスは、USBリダイレクトに使用できます。 USBリダイレクト後、マウスカーソルやキーボードがセッション外で動作しなくなることがあります。 Surface Proタイプカバーおよびタッチカバーデバイスをリダイレクトしないようにする拒否ルールがインストール時に追加されるようになりました。 このルールの動作ついて詳しくは、CTX137939を参照してください。

  注：現在の修正は、Receiverの新規インストールのみに制限されています。 アップグレードの場合は、次の拒否ルールを以下のレジストリに手動で追加する必要があります。

  32ビットOSの場合：
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

  64ビットOSの場合：
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

  DeviceRules値を編集して、USBデバイス固有の拒否ルールを追加します。
  DENY:vid=045e pid=079A（Microsoft Surface Pro 1タッチカバー）
  DENY:vid=045e pid=079c（Microsoft Surface Pro 1タイプカバー）
  DENY:vid=045e pid=07dc（Microsoft Surface Pro 3タイプカバー）
  DENY:vid=045e pid=07e4（Microsoft Surface Pro 4タイプカバー、指紋リーダー付き）
  DENY:vid=03eb pid=8209（Surface Pro Atmel maXTouch Digitizer）

  リダイレクトの拒否を保証するこれらのデバイスのVIDとPIDを追加することで、同じ手順に従います。
  特定のデバイスのDENY: vid=xxxx pid=xxxxルールは、DeviceRules値の一覧の先頭に記述する必要があります。

  [#LC4992]

HDX MediaStream

- ローカルアプリケーションアクセスセッション内でInternet Explorerを開いてFlashコンテンツを含むWebページを参照したときに、アプリケーションが開かれて最大化されていた場合、ブラウザーのFlashコンテナーの内容が画面に残ったままになります。

  [#LC4527]

インストール、アンインストール、アップグレード

- Knowledge CenterのアーティクルCTX135438の指示に従うと、［アカウントの追加］ウィンドウを非表示にしようとしてできないことがあります。 この修正では、Citrix Receiverをリセットまたは再起動した後に［アカウントの追加］ウィンドウを閉じても、再度ポップアップ表示されることがあります。

  [#LC4593]

キーボード

- 公開アプリケーションでCtrl+Alt+「キー」の組み合わせのショートカットキーを使用する場合で、Alt+「キー」またはCtrl+「キー」がCitrixのショートカットキーでもある場合は、この組み合わせがサーバーに送信されません。

[#LC3592]

- シームレスセッションまたはアプリケーションを使用しているときに、マウスクリックが期待したとおりに機能しないこ
  があります。

  [#LC4779]

ローカルアプリケーションアクセス

- Mozilla Firefoxポータブルブラウザー用のURLリダイレクトプラグインをインストールした後、ブラウザーの下部に大きな
  白いボックスが表示されることがあります。

  [#LC4351]

- セッション中にブラウザーを登録または再登録するためにredirector.exeを実行すると、ほとんどのユーザーにとって有用で
  ない情報がポップアップウィンドウに表示されます。 この機能拡張により、redirector.exeコマンドを/verboseオプション
  を指定して実行しない限り、このポップアップウィンドウは表示されなくなりました。

  [#LC4480]

- ローカルアプリケーションアクセスを有効にした公開デスクトップを接続すると、セッションウィンドウが応答しないか表
  示されなくなることがあります。

  [#LC4689]

- Citrix ReceiverでローカルアプリケーションアクセスとUSBリダイレクトの両方を有効にすると、CDViewer.exeプロセスが応
  答しないことがあります。

  [#LC5018]

印刷

- EMFプリンタードライバーで埋め込み記号を含むフォントを使用すると、フォントの埋め込みに失敗することがあります。

  [#LC3334]

シームレスウィンドウ

- シームレスアプリケーションを起動後に最小化すると、タスクバーから復元または最大化できません。

  [#LC3990]

セッション/接続

- WPADを使用するプロキシをまたぐセッションが適切に再接続されません。 切断されたセッションに再接続すると、次の
  ようなメッセージが表示されます。「アプリケーションへのネットワーク接続が中断されました。 後でアプリケーション
  へのアクセスを試すか、ヘルプデスクに問い合わせてください。」

  [#LC3077]

- あるリージョンの信頼済みサイトの特定の構成とは異なるリージョンにStorefront URLを追加しても、機能しません。

  [#LC3281]

- ローカルファイルタイプの関連付けを使用するには、次のレジストリキーを使用します。 次のレジストリキーは、デフォ

ルトではtrueに設定されています。 キーがtrueに設定されていて、クライアントマシン上のそのファイルに他のプログラムが関連付られていない場合は、ローカルファイルのアイコンはCitrix Receiverのアイコンに変更されます。
HKEY_CURRENT_USER\Software\Citrix\Dazzle\EnabledDefaultFTAs=false (REG_SZ)

[#LC4096]

- セッション画面の保持と自動クライアント再接続のタイムアウトが切断された後、セッションの起動が遅れ、セッション共有が機能しません。

  [#LC4143]

- マップされたクライアントドライブのサイズが誤って表示され、1TBを超えている場合は、そのドライブにファイルをコピーできません。 この修正により、ドライブが1TBを超えている場合にも0.99TBと表示されるようになりました。 マップされたクライアントドライブのサイズは、従来のクライアントドライブマッピングオプションを有効にしているときにのみ、表示されます。

  [#LC4214]

- ローカルアプリケーションアクセス（Local App Access：LAA）とDesktop Lockを有効にしていると、全画面の公開サーバーデスクトップセッションへの再接続が原因で、セッションのフォーカスが失われて応答しなくなることがあります。

  [#LC4253]

- Windowsのログオンオプションの「ユーザーの切り替え」を使用すると、仮想デスクトップのセッションの解像度が変更されます。

  [#LC4452]

- Citrix Receiverを使用しているときに、ICO SDKでアプリケーションを起動できないことがあります。

  [RcvrForWin4.4_14.4.1000から][#LC4550]

- ユーザーがSelf Service Plug-inを介してStoreFrontにログオンすると、SelfService.exeプロセスが、毎時間、断続的に他のアクティブなウィンドウのフォーカスを奪います。

  [#LC4628]

- ネットワーク間を移行すると、Epicアプリケーションのフォーカスが失われることがあります。

  [#LC4731]

- アプリケーションを起動しようとすると、wfica32.exeプロセスが予期せず終了することがあり、「への接続に失敗しました。状態（不明なクライアントエラー0)」というエラーメッセージが表示されます。

  [#LC4768]

- NotificationDelayレジストリ設定では、シームレス接続での接続の進行状況バーの表示遅延を管理します。 SelfService Pluginを使用してアプリケーションを起動するときに、このレジストリの設定が機能しないことがあります。 この修正によりその問題が解決されます。

  32ビットWindows：
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  値の名前：NotificationDelay
  種類：REG_DWORD

値のデータ：<遅延（ミリ秒） in milliseconds>

64ビットWindows：
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
値の名前：NotificationDelay
種類：REG_DWORD
値のデータ：<遅延（ミリ秒） in milliseconds>

[#LC4969]

システムの例外

- GPOを使用してXenAppサービスのURLを更新し、新しいGPOを適用するか、同じGPOを新しいストア値（store1、store2など）で更新すると、Citrix Receiver for Windowsが予期せず終了することがあります。

  [#LC4145]

- wfica32.exeプロセスで、アクセス違反が発生して、予期せずに終了する場合があります。

  [#LC4482]

- SelfService.exeプロセスによりCPUが100%使用されることがあります。

  [#LC4494]

- エンドポイントでGPUスイッチを有効にしたセッションが応答しなくなることがあります。

  [#LC4562]

ユーザーエクスペリエンス

- この修正により、クライアントオーディオのリアルタイムモードを使用して短時間再生されるサウンドのサポートが強化されます。 この修正は、低音質のみに適用されます。

  [#LC2783]

- XenApp 7.5で、Windowsのシステムサウンドが聞こえなくなることがあります。

  [#LC3926]

- ネットワーク環境が不安定なときに、「現在アプリケーションを使用できません。 しばらく待ってから再試行してください。または、ヘルプデスクに連絡してこの情報を知らせてください。にアクセスできません」と「アプリケーションへのネットワーク接続が中断されました。 後でアプリケーションへのアクセスを試すか、ヘルプデスクに問い合わせてください。」というメッセージがポップアップ表示されます。 この修正では、ポップアップメッセージを無効にできる、以下のレジストリキーのサポートが追加されました。

  32ビットWindows：
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
  値の名前：SuppressDisconnectMessage
  種類：REG_DWORD
  値のデータ：24(0x18)

  64ビットWindows：
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle

値の名前：SuppressDisconnectMessage
種類：REG_DWORD
値のデータ：24(0x18)

[#LC4378]

ユーザーインターフェイス

- ショートカットを手動で削除してからアプリケーションを更新すると、ショートカットが再表示されないことがあります。

  [#LC4020]

Receiver for Windows 4.4

Citrix Receiver for Windows 4.3.100との比較

Receiver for Windows 4.4には、Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100、4.1.200、4.2、4.2.100、4.3、および4.3.100に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

インストール、アンインストール、アップグレード

- Citrix Receiverをアンインストールした後、Citrix HDX WMI Providerが機能しないことがありました。

  [#LC3943]

キーボード

- セッション画面の保持を有効すると、Snap-to機能が再接続セッションでは機能しません。 Snap-to機能は、**[コントロールパネル]** > **[マウス]** > **[ポインターオプション]** > **[ポインターを自動的に既定のボタン上に移動する]** でマウス/キーボード設定を構成します。

  [#LC1252]

- Alt+Tabキーを使ってウィンドウを切り替えると、公開デスクトップのアプリケーションメニューがアクティブになります。

  [#LC2947]

- Citrix ReceiverとRDPセッションは同じキーボードショートカット"Ctrl+Alt+End"キーを共有してターミナルセッション内で"Ctrl+Alt+Delete"キーを呼び出します。 この結果、Citrix Receiverセッション内で実行している場合はRDPセッションの

キーボードショートカットが機能しません。

この修正により、"Ctrl+Alt+End"キーのキーボードショートカットはCitrix Receiverセッションのデフォルトキーではなく、次のレジストリキーを設定して有効にできます。

- 32ビットWindows：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  値の名前：EnableCtrlAltEnd
  種類：REG_DWORD
  値のデータ：1

- 64ビットWindows：

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  値の名前：EnableCtrlAltEnd
  種類：REG_DWORD
  値：1（値が0の場合、Ctrl+Alt+EndキーはRDPセッションに適用されます）

[#LC3131]

- Citrix Receiverをバージョン4.2にアップグレードした後、ダブルホップシナリオでマウスをクリックすると正常に機能しません。

  [#LC3770]

ローカルアプリケーションアクセス

- ローカルアプリケーションアクセスを有効にして、仮想マシン上のセッションのリサイズのためにマウスをクリックすると、仮想マシンのレンダリングが応答しなくなります。

  [#LC1853]

ログオン/認証

- 資格情報のキャッシュされた完全修飾ドメイン名（FQDN）を使ってログオンしようとするとシングルサインオンが機能しないことがあります。

  [#LC3305]

- 公開デスクトップセッションでWeb InterfaceまたはStoreFrontサーバーに対してパススルー認証を使用するようにReceiverを構成すると、Receiverが資格情報を渡さないで資格情報の入力を求められることがあります。

  [#LC3388]

セッション/接続

- セッションの事前起動を構成して、公開アプリケーションを実行しているセッションに再接続しようとすると、公開アプリケーションの追加のインスタンスが同じセッションに追加されます。

  [#LC1701]

- フォアグラウンドで実行中のWindowsセッションが、予期せずにフォーカスを失う場合があります。

[#LC2198]

- レジストリハイブ**HKEY_LOCAL_MACHINE\SOFTWARE\\Citrix\AuthManager**でポリシー**ProxyEnabled = false**に設定して、IEで構成されたプロキシサーバーを省略します。 32ビットOSアーキテクチャを使用すると、**Wow6432Node**ハイブは適用されません。

  [#LC3129]

- オーディオおよびビデオデータが別個のポートで構成されるマルチポートまたはマルチストリーム構成では、オーディオがビデオと同期とされないことがあります。

  [#LC3181]

- スマートカードでReceiver 4.2 for Windowsに認証されるユーザーは、XenApp公開アプリケーション起動するとPIN認証を求められることがあります。

  [#LC3187]

- 公開アプリケーションの"KEYWORDS:prefer"構成が機能しないことがあります。 これは、ユーザーがReceiverをログオフしてSelfService.exeプロセスが予期せず閉じた場合に発生します。

  [#LC3190]

- Citrix Receiverにログオンした後、ユーザーデバイスの［スタート］メニューとデスクトップにアプリケーションショートカットが表示されるまで時間がかかることがあります。

  [#LC3323]

- Microsoft Outlookの公開インスタンスでメールメッセージからWindowsメディア（.wmv）ビデオを開こうとすると失敗することがあります。

  [#LC3453]

- Desktop Viewerを全画面モードからウィンドウモードに切り替えると、Receiverを使用している間にXenDesktopセッションにフリーツールバーが表示されることがあります。

  [#LC3526]

- Desktop LockとReceiver 4.3をインストールしたシステムがロックされると、デスクトップセッションがアクティブのままになるのではなく、切断することがありました。

  この修正を有効にするには、以下のレジストリキーを設定します。

  - 32ビットWindows：

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
    値の名前：LiveInDesktopDisconnectonLock
    種類：REG_SZ
    値：False
  - 64ビットWindows：

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle
    値の名前：LiveInDesktopDisconnectonLock

種類：REG_SZ
値：False

[#LC3579]

- Citrix Offline Plug-inがインストールされていないCitrix Receiverのクライアントにストリーム配信されたアプリケーションサブスクライブされている場合は、Citrix Receiver内でアプリケーションを更新している間に次のエラーメッセージが表示されることがあります。

  「現在アプリケーションを使用できません」

  [#LC3609]

- Citrix Receiver for Windowsでログオンすると、異なるワーカーサーバー上の複数の事前起動セッションに同じユーザーの同じデリバリーグループに表示されることがあります。

  [#LC3676]

- マルチモニターセッションでThomson Reuters Eikonツールバーのドックを解除した後、ツールバーが占用してしたスペースはセッションに回復されません。

  [#LC3773]

- デバイスにバージョン4.3よりも前のReceiver for WindowsがインストールされていてユーザーがオペレーティングシステムをWindows 7、Windows 8、またはWindows 8.1からWindows 10にアップグレードすると、［プログラムの追加と削除］を介するReceiverのアンインストールに失敗することがあります。 Receiver for Windows 4.3へのアップグレードにも失敗します。

  [#LC3789]

- 新しいセッションを開始しようとすると、wfica32.exeプロセスが予期せず終了することがあります。

  [#LC3795]

- Citrix Receiverを介して公開デスクトップからアプリケーションを開き、"%appdata%"フォルダーを別のファイルサーバーに変更すると、次のエラーメッセージが表示される場合があります。

  「エラー1046：仮想ドライバーが読み込まれていません」

  [#LC3981]

- Lotus Notesのローカルにインストールされたインスタンスのアラームウィンドウは公開アプリケーションからキーボードフォーカスを取得します。

  [#LC3889]

- スタートメニューとデスクトップ上の両方のカテゴリフォルダーにアイコンが表示されることがあります。 デスクトップにはカテゴリフォルダーが存在する必要がありません。 スタートメニューとデスクトップの両方のカテゴリフォルダーにあるコントロールアイコンにレジストリキー"UsCategoryAsStartMenuPath"を使用すると問題が発生します。

  この修正を有効にするには、以下のレジストリキーを設定する必要があります。

  - レジストリキー"UseDifferentPathsforStartmenuAndDesktop"を"false"に設定すると、
    キー"UseCategoryAsStartMenuPath"はスタートメニューとデスクトップの両方に対するカテゴリフォルダーの作成を制

御します。
- レジストリキー"UseDifferentPathsforStartmenuAndDesktop"を"true"に設定すると、
  キー"UseCategoryAsStartMenuPath"はスタートメニューのアイコンカテゴリフォルダーの作成を制御します。
  キー"UseCategoryAsDesktopPath"はデスクトップ上のアイコンカテゴリフォルダーの作成を制御します。

[#LC4052]

- Citrix Receiverでパスワードを変更しようとすると、次のエラーメッセージが表示されることがあります。

  「入力した古いパスワードが正しくありません。」

  [#LC4081]

システムの例外

- Microsoft AX Dynamics 2009またはExcel 2007を使用している間に、Citrix Receiver 4.xが予期せず終了して次のエラーメッセージが表示されることがあります。

  「Citrix HDX Engineが動作を停止しました」

  [#LC3776]

ユーザーエクスペリエンス

- Citrix Receiverセッションでデスクトップに対するアイコンショートカットを追加しようとすると、いくつかのアイコンがアプリケーション特定のアイコンを表示しないことがあります。 代わりに汎用ホワイトページアイコンが表示されます。

  [#LC4097]

- "EnableFTU"を"false"に設定した場合でも、CItrix Receiver接続ウィザードを無効にできません。

  接続ウィザードが表示されるのを防ぐには、次の順に選択してEnableFTUポリシー設定をReceiver.adm/Receiver.admxを使って無効にします。

  [コンピューターの構成] > [管理用テンプレート] > [Citrix Component] > [CitrixReceiver] > [SelfService] > [EnableFTU]

  [#LC4133]

ユーザーインターフェイス

- Mozilla Firefoxブラウザー用のURLリダイレクトプラグインをインストールした後、ブラウザーの下部に大きな白いボックスが表示されることがあります。

  [#LC3409]

- シームレスレジストリフラグ"ENABLE COLOR SYNC"が設定されたら、シームレスセッションがユーザーデバイスからいくつかの色を継承するのに失敗し、代わりに黒が表示されます。

  この修正を有効にするには、以下のレジストリキーを設定します。

  HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/Citrix/wfshell/TWI
  値の名前：SeamlessFlags
  種類：REG_DWORD

値：0x10

[#LC3768]

- StoreFront URLを変更する場合、Citrix Receiver Self-service Plug-inユーザーインターフェイスを開いてから閉じると、無効と設定されたアプリケーションが選択不可なものとして表示される代わりにゴーストアイコンとして表示されることがあります。

  [#LC3863]

- 特定のアプリケーションで断続的に列挙に失敗することがあります。アプリケーションに関連付けられたアイコンの代わりに空白のアイコンが表示されます。

  [#LC4065]

- Citrix Studioで公開アプリケーションのアイコンを変更したら、そのアプリケーションのデスクトップショートカットは更新されません。

  [#LC4124]

その他

- アカウントをプロキシの背後にあるコンピューター上のCitrix Receiverに追加する場合、Citrix Receiverはビーコンへのアクセス時にプロキシ設定を使用しません。場所は内側や外側でなく、なしと設定されます。

  [#LC2100]

- レジストリ値"ConnectionCenter"を次のキーから削除すると、Citrix Receiverが強制的に修復されます。

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

  [#LC3751]

注：このバージョンのCitrix Receiverには、バージョン4.3、4.2、4.1、および4.0に含まれているすべての修正が入っています。

Citrix Receiver for Windows 4.4の既知の問題

Jan 27, 2017

Citrix Receiver for Windows 4.4 CU3（4.4.3000）の既知の問題

このリリースでは、Citrix Receiver for Windows 4.4、4.4 CU1（4.4.1000）、4.4 CU2（4.4.2000）の既知の問題とともに以下の問題が確認されています。

- ACR/SRのタイムアウト後、Citrix Receiverを終了できないことがあります。 この問題を回避するには、Citrix Receiverからログオフして再ログオンするか、wfcrun32プロセスを終了してください。 [#336、#4115]

Citrix Receiver for Windows 4.4 CU2（4.4.2000）の既知の問題

このリリースでは、Citrix Receiver for Windows 4.4および4.4 CU1（4.4.1000）の既知の問題とともに以下の問題が確認されています。

- 「リモートデスクトップセッションでDesktop Viewerのツールバーを使用せずに公開デスクトップを起動した場合、「全画面モードを終了している」ことを示すツールチップダイアログボックスが表示されないことがあります。 「Shift+F2」キーボードショートカットを使用すると、セッションウィンドウのタイトルバーの表示を制御できます。 回避策として、Shift+F2キーを押してデスクトップを表示してから、セッションウィンドウを最小化してください。」

  [#LC4445、#639585]

Citrix Receiver for Windows 4.4 CU1（4.4.1000）の既知の問題

このリリースでは、Citrix Receiver for Windows 4.4の既知の問題とともに以下の問題が確認されています。

- Citrix Receiver for Windowsをアンインストールした後に、レジストリキー HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\（32ビットシステム上）および の HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\（64ビットシステム）のレジストリ値 "Installer" が削除されません。

  [#635242]

Citrix Receiver for Windows 4.4の既知の問題

このリリースでは、以下の既知の問題が確認されています。

- Windows 10 Surface Proデバイス上でホストされているアプリケーションの方向を変更すると、「全画面モードを終了している」ことを示すツールチップ画面が表示されます。 この問題を回避するには、以下のレジストリキーを設定してヒントダイアログメッセージを無効にします。

  HKEY_CURRENT_USER\Software\Citrix\ica client\keyboard mappings\tips

  値を1にするとヒントが無効になり、0にすると有効になります。このレジストリキー値を1に設定してすべてにヒントを無効にします。

  [#608346]

警告

> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

- Windows 7クライアント上のVDAセッションでは、画面テキストの後ろに白い影が出るという表示の問題があることがあります。 この問題が発生するのは、クライアントに最新のGFXドライバーがインストールされていない場合です。 古いNVIDIAドライバーがインストールされているクライアントでこの問題を解決するには。

  古いNVIDIAドライバーがインストールされているクライアントでこの問題を解決するには：

  1. NVIDIAコントロールパネルにアクセスします。
  2. ［Video settings］へアクセスします。
  3. ［How do you make color adjustments?］セクションで、［With NVIDIA Settings］を選択します。
  4. ［NVIDIA settings］で［Advanced］タブを選択します。
  5. ［Advanced］タブをクリックし、Dynamic Rangeを［Full (0-255)］に設定します。

  クライアントマシンを最新のGFXドライバーで更新するとこの回避策をスキップできます。

  [#610197]

> ## 注意
>
> NVIDIAドライバーの使用については、NVIDIAサポートサイトのDynamic RGB Range Capabilityページを参照してください。

- クライアントでハードウェアデコードが有効な場合にH.264 GraphicsモードでWindows 2008 R2 VDAに接続すると、パフォーマンスが低下します。 この問題を避けるには、VDAでレガシーグラフィックモードを使用することをお勧めします。

  [#609292、611580]

- クライアントで切断/再接続サイクルを複数回繰り返した後、ACRはセッションに再接続せず、ユーザーがStoreFrontに再度ログインする必要があります。

  [#567938]

- NetScaler Gateway End Point Analysis Plugin（EPA）はネイティブのWindows Receiverをサポートしません。

  [#534790]

- 匿名ユーザーセッションを閉じたときに、匿名ログインに当てはまらないメッセージがDesktop Viewerに表示されます。 このような場合、匿名ユーザーがセッションを切断すると、Receiverによりユーザーは自動的にログオフされます。 そのようなログインには認証がないため、匿名セッションでは再接続、クライアント間のローミング、およびワークスペースコントロールはサポートされません。

  [#481561]

- ローカライズされた環境の一部で（中国語でCitrix Receiverを実行するなど）、ローカライズされたログイン資格情報のユーザー名にサロゲートペアが含まれる場合、仮想デスクトップおよびアプリが起動しないことがあります。

  [#556174]

- ドメイン管理者としてReceiverをインストールすると、インストール中に［カスタマーエクスペリエンス向上プログラムテキストの有効化］オプションを選択しいても、［バージョン情報］メニューの［カスタマーエクスペリエンス向上プログラム］ウィンドウを選択できません。

[#556179]

- RAVEとの互換性の問題のため、セッション内のRealTimes（Real Player）でボリュームコントロールが機能しないことがあります。

  [#573549]

- オフラインモードを使用中にReceiverで以下の問題が発生します。
  - ネットワーク接続が失われてもユーザーに状況を知らせるエラーメッセージが表示されません。 オフラインモードでReceiverを使用しているときは、アプリ
    更新、サブスクライブ、サブスクリプションの解除ができません。 [#559792、#560091、#560360]
  - Receiverがオフラインの間にアプリまたはデスクトップに加えられた変更が、ネットワーク接続の再確立後も同期されません。 [#560362]

- Receiverからログアウトして再ログインすると、ユーザー名がインターフェイスの右上に表示されません。

  [#562107]

- スマートカード認証がXenApp Servicesサイトで機能しませんが、StoreFrontサイトでは機能します。 この問題を解決するには、スマートカード認証をStoreFront
  サイトで設定してください。

- たとえば**TLS and Compliance Mode Configuration**などのユーザーインターフェイスのフィールドラベル上で、SSLへのリファレンスがまだ見られる場合があり
  ます。 この問題は、将来のリリースで更新されます。

- Desktop Lockクライアントのログオン画面に言語バーが表示されません。 解決策として、浮動言語バーを使用します。

  [#502678]

- セッションをウィンドウモードで開くと、Citrix Desktop Viewerの［ショートカット］オプションが機能しません。

  [#510529]

- 匿名ユーザーセッションに対しては、切断時のDesktop Viewerのアラートメッセージが表示されません。 これは仕様です。

  [#481561]

- Receiver for Windowsは、ユーザー（非管理者）アカウントではWindows Server 2012 R2マシンにインストールできません。

  この問題を解決するには、次の手順に従います。

  1. **［スタート］**をクリックして「**regedit**」と入力し、**Enter**キーを押します。
  2. 次の設定を見つけます。

  HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer

  Create: DisableMSI Type: REG_DWORD value = 0（0に設定するとインストールできます）

  [#492508]

- システムトレイ通知がデスクトップロックモードで見られることがあります。

  [#488620]

- ターミナルサーバーVDAでは仮想キーボードが自動的に表示されません。 Desktop Viewerツールバーのアイコンを使って、またはアプリケーションの場合はタス
  クバー上の仮想キーボードアイコンから仮想キーボードを開く必要があります。

  [#502774]

- 汎用USBでUSBヘッドセット（Logitech USB H340）をリモート操作する場合、通常よりも音質が低下します。 これは仕様です。 オーディオ最適化はUSBのリタ
  イレクトでは実行されません。 この機能は、将来のリリースでの強化が検討されています。

  [#469670]

- 7.0よりも前のバージョンのXenAppおよびXenDesktop、またはWindow 2008 R2上のXenAppおよびXenDesktop 7.0以降を介してリモート操作されるアプリケー
  ションでは、ピンチおよびズームジャスチャーは機能しません。

[#517877]

システム要件と互換性

Sep 19, 2016

デバイス

オペレーティングシステム

- Windows 10
- Windows 8.1 32ビット版および64ビット版（Embeddedエディションを含む）
- Windows 8 32ビット版および64ビット版（Embeddedエディションを含む）
- Windows 7 32ビット版および64ビット版（Embeddedエディションを含む）
- Windows Vista 32ビット版および64ビット版
- Windows Thin PC
- Windows Server 2012 R2、Standard、およびDatacenterエディション。
- Windows Server 2012、Standard、およびDatacenterエディション。
- Windows Server 2008 R2 64ビット版
- Windows Server 2008 32ビット版および64ビット版

ハードウェア

- VGAまたはSVGAビデオアダプターとカラーモニター
- Windows互換のサウンドカード（サウンドをサポートする場合）
- サーバーファームへのネットワーク接続用のネットワークインターフェイスカードとネットワークトランスポートソフトウェア
- グラフィックパフォーマンスをより良いものにするため、クライアントマシンに最新のGFXドライバーをインストールしておく必要があります。

タッチ操作可能なデバイス

Citrix Receiver for Windows 4.4は、XenAppおよびXenDesktop 7以降がインストールされたWindows 7および8.1が動作するタッチ操作可能なラップトップ、タブレット、およびモニター、ならびにVirtual Desktop Agentがインストールされた Windows 7、8、および2012が動作するコンピューターで使用できます。

Citrixサーバー

- XenAppの以下のバージョン：
  - Citrix XenApp 7.6
  - Citrix XenApp 7.5
  - Citrix XenApp 6.5 Feature Pack 2 for Windows Server 2008 R2
  - Citrix XenApp 6.5 Feature Pack 1 for Windows Server 2008 R2
  - Citrix XenApp 6.5 for Windows Server 2008 R2
  - Citrix XenApp 4 Feature Pack 2 for UNIX operating systems
- XenDesktopの以下のバージョン：
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7.0
- Citrix VDI-in-a-Box
  - VDI-in-a-Box 5.3
  - VDI-in-a-Box 5.2
- StoreFront Receiver for WebとWeb Interfaceとともに、NetScaler Gatewayのプラグインがあってもなくても Citrix

Receiver for Windows 4.4のブラウザーベースのアクセスを実行できます。
StoreFront：
- StoreFront 3.0.x、2.6、2.5、および2.1
  StoreFrontストアへの直接アクセスを提供します。
- Receiver for WebサイトがStoreFront
  StoreFrontストアへのWebブラウザーからのアクセスを提供します。 この場合の制限事項については、「Receiver for Webサイト」の「重要な注意事項」を参照してください。

NetScaler VPNクライアントを使用する場合のWeb Interface：
- Web Interface 5.4.x for WindowsのWebサイト。
  デスクトップやアプリケーションへのWebブラウザーからのアクセスを提供します。
- XenApp ServicesサイトまたはXenDesktop WebサイトをWeb Interface 5.x for Windows

- Citrix Receiverをユーザーに配布する方法：
  - ユーザーによるreceiver.citrix.comからのダウンロードを有効にして、StoreFrontとともにメールまたはサービスアドレスの使用を構成します。
  - Citrix Receiver for Webサイト（StoreFrontと共に構成済み）からのインストールを提供します。
  - Citrix Web Interface 5.4からのReceiverのインストールを提供します。
  - Active Directory（AD）グループポリシーオブジェクト（GPO）を使って展開します。
  - Microsoft System Center 2012 Configuration Managerを使って展開します。

Webブラウザー

- Internet Explorer
  Citrix Receiver for WebまたはWeb Interfaceへの接続は、32ビットモードのInternet Explorerをサポートします。 サポートされるInternet Explorerのバージョンについては、「StoreFrontのシステム要件」および「Web Interfaceのシステム要件」を参照してください。

- Mozilla Firefox 18.x以降
- Google Chrome 20または21（StoreFrontが必要）。

> **注意**
>
> Google Chrome NPAPIサポートへの変更について詳しくは、Citrixのブログアーティクル「Preparing for NPAPI being disabled by Google Chrome」を参照してください。

接続性

Citrix Receiver for Windowsでは、以下の構成のいずれかを介して、HTTP、HTTPS、およびICA-over-TLS接続を確立できます。

- LAN接続の場合：
  - StoreFront ServicesサイトまたはCitrix Receiver for Webサイトを使用するStoreFront。
  - Web InterfaceサイトまたはXenApp Serviceサイトを使用するWeb Interface 5.4 for Windows。

  デバイスがドメインに属している場合と属していない場合について詳しくは、XenDesktop 7のドキュメントを参照してください。

- セキュリティ保護されたリモートまたはローカルの接続の場合：
  - Citrix NetScaler Gateway 11.x
  - Citrix NetScaler Gateway 10.5

Windowsドメイン参加、管理されたデバイス（ローカルおよびリモート、VPNありまたはなし）およびドメイン非参加デバイス（VPNありまたはなし）がサポートされます。

StoreFrontでサポートされるNetScaler GatewayおよびAccess Gatewayのバージョンについては、「StoreFrontのシステム要件」を参照してください。

> **注意**
>
> このトピックに記載されているNetScaler Gatewayについての説明は、特に注記のない限りはAccess Gatewayにも該当します。

セキュリティが保護された接続と証明書について

> **注意**
>
> セキュリティ証明書については、「セキュリティで保護された接続」および「セキュリティで保護された通信」を参照してください。

プライベート（自己署名）証明書

リモートゲートウェイにプライベート証明書がインストールされている場合は、組織の証明機関のルート証明書をユーザーデバイスにインストールしないと、Citrix ReceiverでCitrixリソースにアクセスできません。

> **注意**
>
> 接続時にリモートゲートウェイの証明書を検証できない場合（ローカルのキーストアにルート証明書が含まれていないため）、信頼されていない証明書の警告が表示されます。 ユーザーが警告に対してそのまま続行することを選択した場合、アプリケーションの一覧が表示されますが、アプリケーションの起動に失敗します。

ユーザーデバイスへのルート証明書のインストール

ユーザーデバイスへのルート証明書のインストール、およびWeb Interfaceでの証明書設定については、「Receiver通信のセキュリティ保護」を参照してください。

ワイルドカード証明書

ワイルドカード証明書は、同一ドメイン内の任意のサーバーで個別のサーバー証明書の代わりに使用します。 Citrix Receiver for Windowsはワイルドカード証明書をサポートしますが、組織のセキュリティポリシーに従って使用する必要があります。 実際には、サブジェクトの別名（SAN）拡張内のサーバー名の一覧に含まれている証明書などのワイルドカード証明書に代わるものを考慮が必要なことがあります。 こういった証明書は、私的証明機関および公的証明機関の両方が発行できます。

中間証明書とNetScaler Gateway

証明書チェーンに中間証明書が含まれる場合は、中間証明書をNetScaler Gatewayのサーバー証明書に追加する必要があります。 詳しくは、「中間証明書の構成」を参照してください。

Authentication

StoreFrontへの接続では、Citrix Receiverで以下の認証方法がサポートされます。

	ブラウザーを使った Receiver for Web	StoreFront Servicesサイト（ネイティブ）	StoreFront XenApp Services サイト（ネイティブ）	NetScalerから Receiver for Web（ブラウザー）	NetScalerから StoreFront Services サイト（ネイティブ）
匿名	はい	はい			
ドメイン	はい	はい	はい	はい *	はい *
ドメインパススルー	はい	はい	はい		
セキュリティトークン				はい *	はい *
2要素（セキュリティトークンがあるドメイン）*				はい *	はい *
SMS				はい *	はい *
スマートカード	はい	はい	いいえ		
ユーザー証明書				はい（NetScalerのプラグイン）	はい（NetScalerのプラグイン）

* デバイス上にインストールされたNetScalerプラグイン有または無

> **注意**
>
> Citrix Receiver for Windows 4.4は、NetScaler GatewayからStoreFrontネイティブサービスを通して2FA（ドメイン+セキュリティトークン）をサポートします。

Web Interface 5.4に接続するため、Citrix Receiverは次の認証方法をサポートします（Web Interfaceではドメインおよびセキュリティトークン認証のため「指定ユーザー」という用語を使用します）：

	Web Interface（ブラウザー）	Web Interface XenApp Servicesサイト	NetScalerからWeb Interface（ブラウザー）	NetScalerからWeb Interface XenApp Servicesサイト
匿名	はい			
ドメイン	はい	はい	はい *	

ドメインパススルー	はい	はい		
セキュリティトークン			はい *	
2要素（セキュリティトークンがあるドメイン）*			はい *	
SMS			はい *	
スマートカード	はい	いいえ		
ユーザー証明書			はい（NetScalerのプラグイン）	

* NetScaler Gatewayが動作する環境でのみ使用できます（デバイスへのゲートウェイプラグインソフトウェアのインストールは不要）。

認証については、eDocsのNetScaler Gatewayのドキュメントの「Configuring Authentication and Authorization」と、StoreFrontのドキュメントで「管理」のトピックを参照してください。 Web Interfaceでサポートされる認証方法については、「Web Interfaceの認証方法の構成」を参照してください。

アップグレード

Citrix Receiver for Windows 4.xでは、Receiver for Windows 3.xと、Citrix Online Plug-in 12.xをアップグレードできます。 アップグレードについて詳しくは、「アップグレード時の注意事項」を参照してください。

> **注意**
>
> Citrix Receiver 3.4からVersion 4.2.100にアップグレードする場合は、「Receiver 3.4からReceiver 4.2.100へのアップグレードガイド」に記載されている手順に従います。 Version 4.2.100ではエンドユーザーによるインプレースアップグレードはサポートされません。 ネットワーク上のすべてのユーザーが正常にアップグレードできるように、IT管理者は環境を準備する必要があります。 アップグレードガイドには詳しい手順が記載されています。

Other

- **.NET Frameworkの要件**
  - Self-Service Plug-inでは.NET 3.5 Service Pack 1が必要となります。ユーザーはこのプラグインを使って、Receiverのウィンドウまたはコマンドラインから仮想デスクトップやアプリケーションへのサブスクライブを実行して起動できます。詳しくは、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」を参照してください。
  - Receiverアイコンを問題なく表示するには、.NET 2.0 Service Pack 1およびMicrosoft Visual C++ 2005 Service Pack 1再頒布可能パッケージが必要です。 Microsoft Visual C++ 2005 Service Pack 1パッケージは、.NET 2.0 Service Pack 1、.NET 3.5、および.NET 3.5 Service Pack 1に含まれており、単独で入手することもできます。
  - XenDesktop接続の場合：Desktop Viewerを使用するには.NET Framework 2.0 Service Pack 1以降が必要です。 インターネットにアクセスできない場合は証明書失効チェックにより接続の起動時間が長くなるため、このバージョンが必要で

す。 このバージョンのFrameworkではチェックを無効にして起動時間を短縮できますが、.NET 2.0ではできません。

- Microsoft Lync Server 2013およびMicrosoft Lync 2013 VDI Plug-in for Windowsとの併用については、「XenDesktop、XenApp、およびCitrix ReceiverでのMicrosoft Lync 2013 VDI Plug-inのサポート」を参照してください。

- **サポートされる接続方法とネットワークトランスポート：**
  - TCP/IP+HTTP
    必要となることがある追加の値については、CTX 134341を参照してください。

  - TLS+HTTPS

> ## Important
>
> StoreFrontで構成された［Transport type］が［HTTP］のストアを使用するには、レジストリキーHKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\AuthManagerにConnectionSecurityMode=Anyを設定する必要があります。

> ## 警告
>
> レジストリエディタの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

インストール

Aug 30, 2016

CitrixReceiver.exeのインストールパッケージは、以下の方法でインストールできます。

- Citrix.comまたは管理者が作成したダウンロードサイトからのインストール
  - Receiverを初めて使用するユーザーがReceiverのインストールファイルをCitrix.comなどのダウンロードサイトから入手した場合は、サーバーURLの代わりにメールアドレスを入力してアカウントをセットアップできます。 これにより、メールアドレスに関連付けられたNetScaler Gateway（またはAccess Gateway）やStoreFrontサーバーが識別され、ログオン用のメッセージが表示されます。ユーザーは、ログオンしてインストールを完了します。 この機能は、「メールアドレスによるアカウント検出」と呼ばれます。
    注：初めて使用するユーザーとは、デバイスにReceiverをインストールしていないユーザーを指します。
  - Citrix.com以外の場所（Receiver for Webサイトなど）からReceiverをダウンロードした場合は、メールアドレスによるアカウントセットアップを使用できません。
  - Receiverの構成が必要な環境では、ほかの方法でReceiverをユーザーに配布してください。
- Receiver for WebサイトまたはWeb Interfaceのログオン画面からの自動インストール
  - Receiverを初めて使用するユーザーがアカウントをセットアップするには、サーバーのURLを入力するかプロビジョニング（CR）ファイルをダウンロードします。
- ESD（Electronic Software Delivery：電子ソフトウェア配信）ツールによるインストール
  - Receiverを初めて使用するユーザーがアカウントをセットアップする場合、サーバーのURLを入力するかプロビジョニングファイルを開く必要があります。

パススルー認証を使用しない場合、Receiverのインストールに管理者権限は不要です。

HDX RealTime Media Engine (RTME)

単一のインストーラーでは、最新のCitrix Receiver for WindowsとHDX RTMEインストーラーが結合されています。 このバージョンのCitrix Receiverをインストールすると、HDX RTMEが実行可能ファイル（.exe）に含まれます。

> **注意**
>
> RTMEサポートが統合された最新バージョンのCitrix Receiverのインストールには、ホストマシンの管理者権限が必要です。

Citrix Receiverをインストールまたはアップグレードする場合は、HDX RTMEに関して次の点のご注意ください。

- 最新バージョンのCitrix Receiverには、最新バージョンのHDX RTME（バージョン1.0.0.1）が含まれているため、別途RTMEをインストールする必要はありません。
- 前バージョンのReceiverから最新のバンドルバージョン(RTMEを含むCitrix Receiver)へのアップグレードに対応しています。 以前インストールされたRTMEのバージョンは、最新バージョンに上書きされます。同じReceiverのバージョンから最新のバンドルバージョンへのアップグレード（例: Receiver 4.4からRTMEがバンドルされたReceiver 4.4）はサポートしていません。
- 以前のバージョンのRTMEをお持ちの場合、最新バージョンのReceiverをインストールすることにより、クライアントデバイスのRTMEも自動的に更新されます。
- 最新バージョンのRTMEがインストール済みであれば、インストーラーはそのバージョンを保持します。

> **Important**

XenApp/XenDesktopサーバー上のHDX RealTime Connectorを最新バージョンの2.0.0.417（GAリリース）にして新しいRTMEパッケージと互換性を持たせる必要があります。RTME 2.0は1.8 RTME Connectorとは使用できません。

Citrix Receiver for Windowsの手動アップグレード

StoreFront環境：

- BYOD（Bring Your Own Device）ユーザー（私的デバイス活用ユーザー）のベストプラクティスについては、製品ドキュメントのサイトでドキュメントを参照しながら最新バージョンのNetScaler GatewayおよびStoreFrontを構成してください。 StoreFrontにより作成されたプロビジョニングファイルをメールに添付して、アップグレード方法およびReceiverのインストール後にプロビジョニングファイルを開く方法をユーザーに通知します。
- プロビジョニングファイルをユーザーに送信できない場合は、NetScaler Gateway（またはAccess Gateway Enterprise Edition）のURLを入力するように指示します。 また、StoreFrontのドキュメントで説明されているメールアドレスによるアカウント検出を構成済みの場合は、自分のメールアドレスを入力するようにユーザーに指示します。
- また、Receiver for Webサイトを構成（StoreFrontのドキュメントを参照）し、「Receiver for WebサイトからのReceiver for Windowsの配布」の説明に従って構成を完了する方法もあります。 Receiverのアップグレード方法、Receiver for Webサイトへのアクセス方法、Receiver for Webサイトからのプロビジョニングファイルのダウンロード方法（ユーザー名をクリックして［アクティブ化］をクリック）をユーザーに通知します。

Web Interfaceで展開する場合

- Receiver for WindowsでWeb Interfaceサイトをアップグレードし、「Web Interfaceのログオン画面からのReceiver for Windowsの配布」で説明されている構成を完了します。 Receiverのアップグレード方法をユーザーに通知します。 たとえば、ユーザーがReceiverインストーラーを入手するためのダウンロードサイトを作成して、そこに名前を変更したインストーラーを配置します。

アップグレード時の注意事項

ヒント

Receiver for Windows 4.xでは、パススルー認証（シングルサインオン）の構成プロセスが変わりました。詳しくは、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」の/includeSSONの説明を参照してください。

Citrix Receiver for Windows 4.xでは、Receiver for Windows 3.xと、Citrix Online Plug-in 12.xをアップグレードできます。

Receiver for Windows 3.xまたはOnline Plug-inがマシン単位でインストールされている場合、管理権限のないユーザーによるユーザー単位のアップグレードはサポートされません。

Receiver for Windows 3.xまたはOnline Plug-inがユーザー単位でインストールされている場合、マシン単位でのアップグレードはサポートされません。

ユーザーによるReceiver for Windowsのインストールとアンインストール

Feb 02, 2016

インストールメディア、ネットワーク共有、Windowsエクスプローラー、またはコマンドラインでCitrixReceiver.exeインストーラーパッケージを手動で実行してReceiverをインストールできます。 コマンドラインでのインストールパラメーターおよびスペースの要件については、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」を参照してください。

> **Important**
>
> Receiver for Windows 4.xでは、パススルー認証（シングルサインオン）の構成プロセスが変わりました。詳しくは、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」の/includeSSONの説明を参照してください。

社内ポリシーでEXEファイルの使用が禁止されている場合は、「How to Manually Extract, Install, and Remove Individual .msi Files」を参照してください。

Receiverの手動インストールおよびパススルー認証の構成

ReceiverはXenAppおよびXenDesktopでパススルー認証を使用するシナリオで使用できます。 またこのセクションでは、Web InterfaceまたはStoreFrontサーバー接続用にパススルー認証を使用するためCitrixReciver.exeをインストールして構成する方法についても説明します。

正常にインストールして構成した場合、ユーザーは資格情報を再入力せずにXenApp/XenDesktopリソースにアクセスできます。 クライアントマシンの資格情報はエンドポイントに自動的にパススルーされます。

パススルー認証を使用する場合、次のことに注意してください。

- Citrix Receiver for WindowsのインストールパッケージはCitrixReceiver.exeです。
- グループポリシーファイルを適宜読み込みます：
  - receiver.adm（Citrix Receiverがインストールされ ているWindowsマシンの%SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configurationフォルダーにある）。receiver.admファイルはWindows XP、Windows 2003、およびシンクライアントに存在します。
  - receiver.admx、receiver.adml （Citrix Receiverがインストールされ ているWindowsマシンの%SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configurationフォルダーにある）。GPOにADMXファイルを読み込むには、「グループポリシーオブジェクトテンプレートによるReceiverの構成」のADMXテンプレートの使用に関する説明を参照してください。
- クライアントデバイスでソフトウェアのインストールや構成を実行するにはローカル管理者権限が必要です。
  注：.admファイルはシンクライアントにXPe OSが実行されている場合にのみ使用されます。

Citrix Merchandising ServerやMicrosoft System Center Configuration Managerのようなエンタープライズソフトウェア展開ツールを使用しない場合は、XenApp/XenDesktopへのパススルー認証を実現するための展開シナリオが2つあります。

1. Citrix Receiverをさまざまなマシンに個別に手動でインストールして、ローカルグループポリシーを使って構成する（receiver.adm、receiver.admx、receiver.admlのインポート）。
   注：このシナリオは非常に小さな環境に推奨されます。

2. Citrix ReceiverをActive Directoryグループポリシーを使用してインストールする（たとえばXenAppに含まれる**CheckAndDeployCitrixReceiverEnterpriseStartupScript.bat**を使用します）。 その後で、**receiver.adm**、**receiver.admx**、**receiver.adml** を使用する構成をActive Directoryのグループポリシーの管理を使って多くのマシンに適用し、集中管理できます。

このオプションは非常に複雑なため、この記事では説明しません。 詳しくは、CTX134280 - 「How to Deploy Citrix Receiver Enterprise for Pass-Through Authentication Using Active Directory Group Policy」を参照してください。

注：この記事で概説するどの手順も、使用する前に非実稼働環境で十分にテストおよび検証することを強くお勧めします。

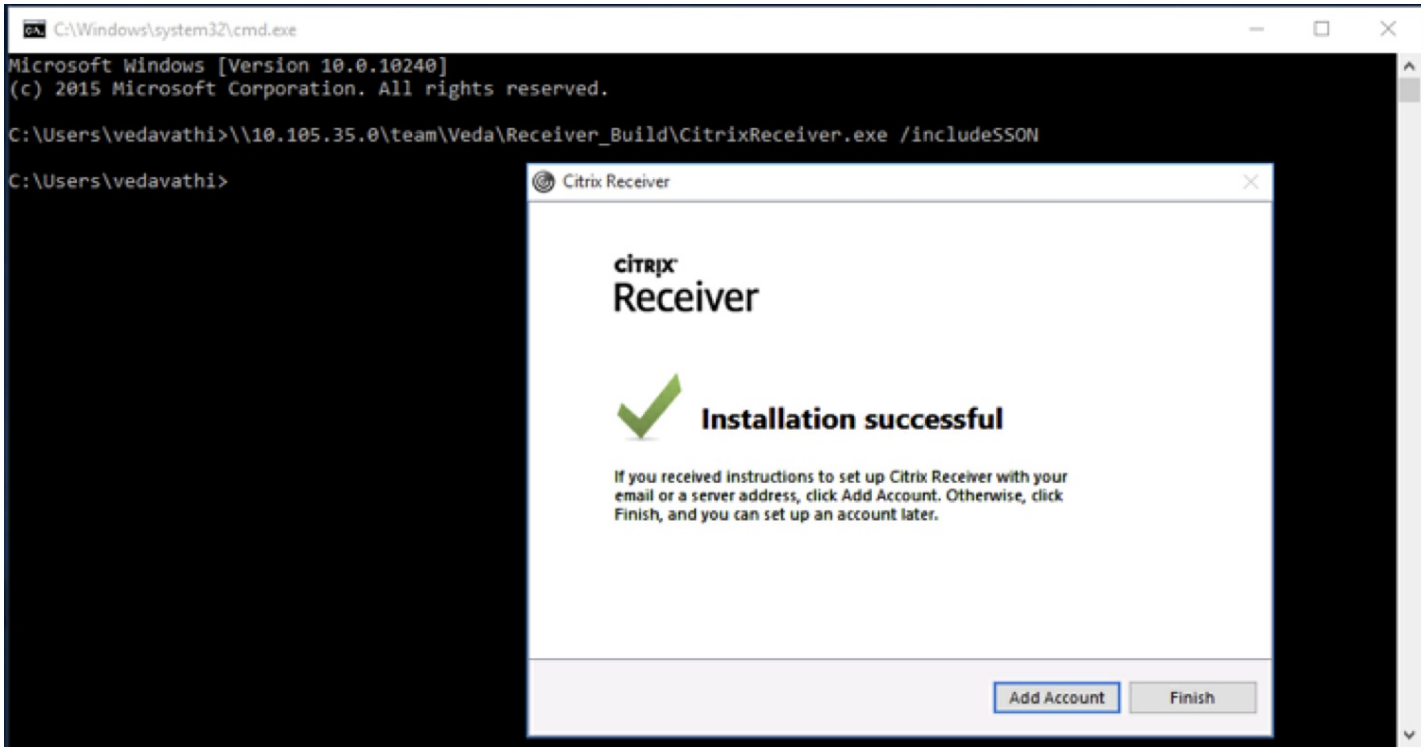
Receiverを手動でインストールしてパススルー認証を構成するには

1. ControllerでPowerShellを使って次のコマンドを実行します :**Set-BrokerSite -TrustedRequestsSentToTheXmlServicePort $True**
2. 管理権限のあるユーザーとしてクライアントマシンにログオンします。
3. インストールを始める前に、既存のOnline PluginまたはCitrix Receiver for Windowsをクライアントマシンからアンインストールします。
4. Citrix Downloadsから Citrix Receiver for Windowsのインストールパッケージ（CitrixReceiver.exe）をダウンロードします。

適切なインストール展開を使用するには、コマンドライン、またはGUIを使用します 。

コマンドラインを使用するには：

1. **Windowsのコマンドプロンプト**を開いて、CitrixReceiver.exeのあるディレクトリに移動します。
2. **コマンドプロンプトで**次のコマンドを実行して、シングルサインオンを有効にしてCitrix Receiverをインストールします：**CitrixReceiver.exe /includeSSON** 「コマンドラインパラメーターを使用したCitrix Receiver for Windowsの構成とインストール」の情報を参照します。パラメーター/includeSSONにより、標準版のReceiver（CitrixReceiver.exe）でシングルサインオンが有効になります。 このオプションは、デフォルトでシングルサインオンが有効なエンタープライズ版のReceiver（CitrixReceiverEnterprise.exe）ではサポートされません。
3. インストールが完了すると「インストールに成功しました」というポップアップメッセージが表示されます。



GUIを使用するには：

1. CitrixReceiver.exeをダブルクリックします。
2. シングルサインオンの有効化インストールウィザードで、シングルサインオンを有効にするチェックボックスをオンにしてCitrix ReceiverでSSON機能を有効にしてインストールします。 これは、コマンドラインで/includeSSONフラグを使ってReceiverをインストールするのと同じです。

注：シングル サインオンの有効化インストールウィザードは、ローカル管理者によりドメイン参加マシンでフレッシュ（新規）インストールをする場合にのみ使用できます。

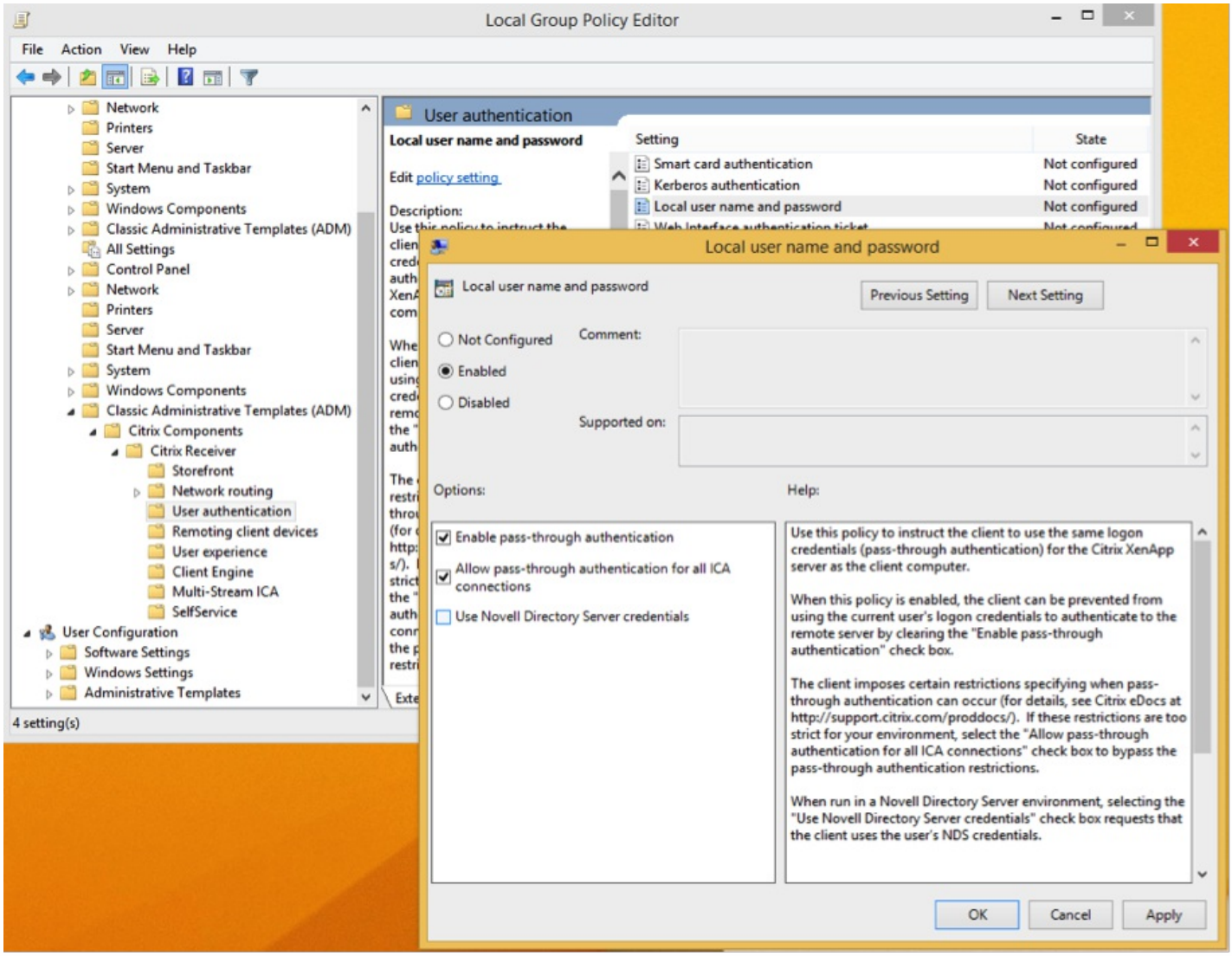
ローカルグループポリシーエディター（GPO）を介したシングルサインオンの構成

デフォルトでは、シングルサインオンのためグループポリシーで**[Enable pass-through authentication]**を有効にします。Desktop ViewerおよびReceiver for Webが使用されていない場合は、これでシングルサインオンが機能します。 Desktop Viewerを使用している場合は、GPOで **[Allow pass-through authentication for all ICA connections]** を有効にします。

ADMファイルを使ってユーザー認証を構成するには

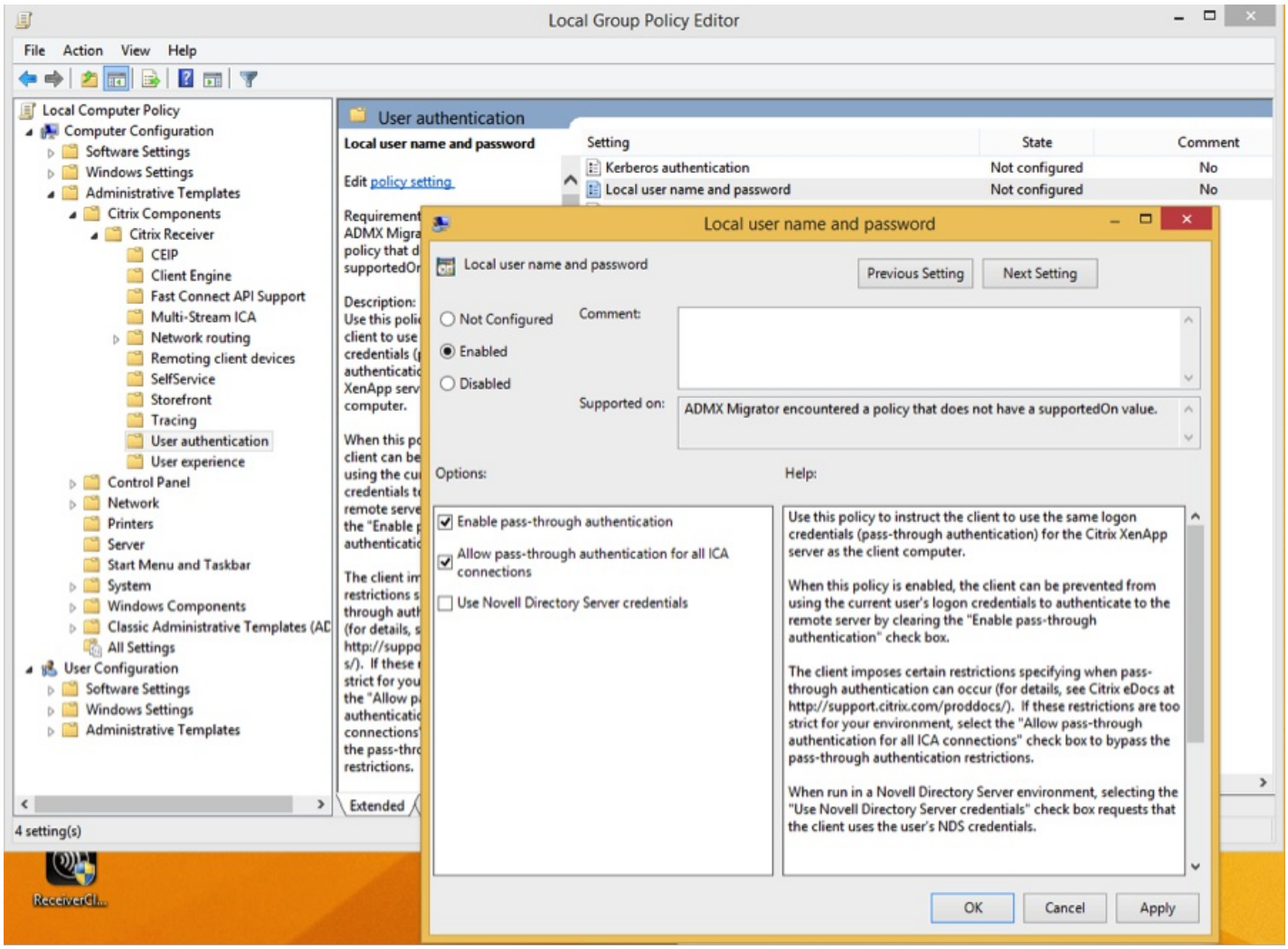
1. ［スタート］メニューで**gpedit.msc**コマンドを実行するか「編集 グループ ポリシー」というキーワードで検索して［ローカルグループポリシーエディター］を開きます。
2. ローカルグループポリシーエディターにreceiver.admテンプレートを追加します。これを行うには、［コンピューターの構成］の［管理用テンプレート］を右クリックし、［テンプレートの追加と削除］を選択して**［追加］**をクリックします。
3. receiver.admテンプレートを問題なく追加したら、［コンピューターの構成］>［管理者テンプレート］>［従来の管理用テンプレート（ADM）］>［Citrix Components］>［Citrix Receiver］>［User authentication］の順に選択します。

注：StoreFrontまたはReceiver for Webの構成およびセキュリティ設定によっては、パススルー認証を実行するために **[Allow pass-through authentication for all ICA connections]** チェックボックスをオンにする必要があります。



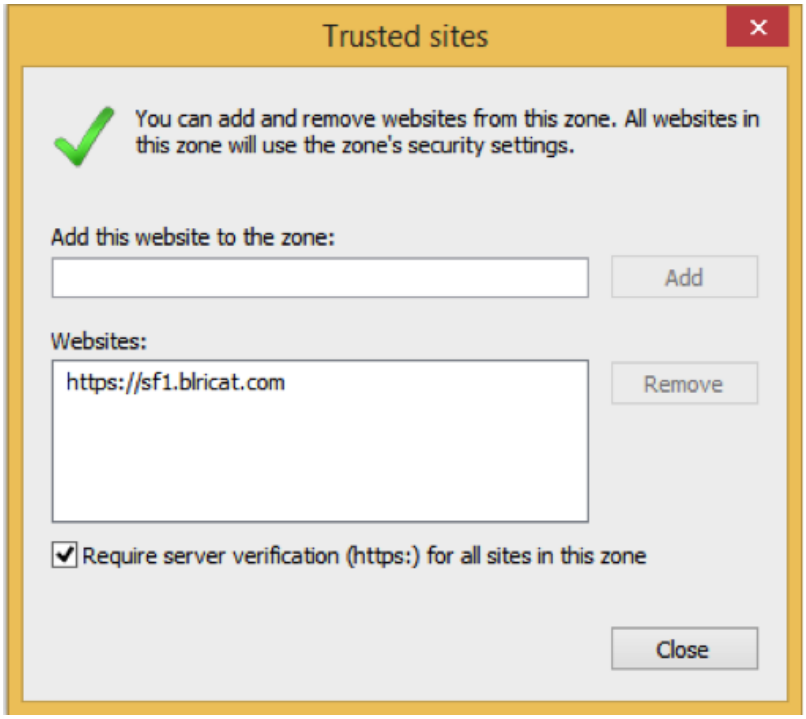
パススルー認証に対するADMXの使用

1. ローカルグループポリシーエディターにreceiver.admxおよびreceiver.admlテンプレートを追加します。 詳しくは、 グループポリシーオブジェクトテンプレートによるReceiverの構成」でADMXテンプレートの使用に関する説明を参照してください。
2. receiver.admxおよびreceiver.admlテンプレートの追加に成功したら、［コンピューターの構成］>［管理者テンプレート］>［Citrix Components］>［Citrix Receiver］>［User authentication］の順に選択します。
3. **［Local user name password］**設定を選択します。
4. ［有効］をクリックして、［Enable pass-through authentication］および［Allow pass-through authentication for all ICA connections］チェックボックスをオンにします。



信頼済みサイト一覧への完全修飾ドメイン名（FQDN）の追加

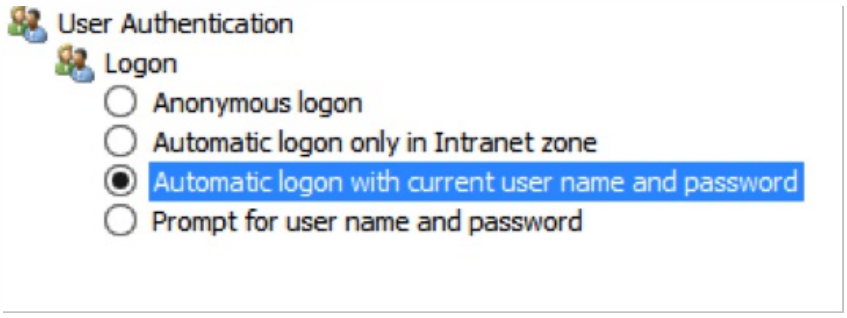
1. クライアントデバイスで、Internet Explorerを起動します。
2. Internet Explorerで、［ツール］>［インターネットオプション］>［信頼済みサイト］の順にクリックします。
3. **［追加］**をクリックして信頼済みサイトの一覧にFQDNを追加します（例：https://sf1.blricat.com）。 追加したら、Webサイトの一覧にサイトが表示されます。



信頼済みサイトの一覧にWebサイトを追加した後、適切なユーザー認証方法を選択します。

1. ［セキュリティ］タブで［信頼済みサイト］を選択します。
2. **［レベルのカスタマイズ］**をクリックします。
3. 一覧の一番下までスクロールして、**［現在のユーザー名とパスワードで自動的にログオンする］**をクリックします。
4. クライアントデバイスを再起動して変更を適用します。

注：［現在のユーザー名とパスワードで自動的にログオン］は、ユーザーごとに適用されます。この設定をローカル管理者が構成しない場合は、各ユーザーがこのオプションを設定する必要があります。この設定を全般的に適用させるには、インターネットと信頼済みサイトの両方で、カスタムレベルにこの値を追加して、GPOを構成します。



シングルサインオン（SSON）を使う場合の重要なアップグレード考慮事項

次の表には、コマンドラインでSSONを使ったReceiverのアップグレードに関する情報が記されています。

アップグレードの前にインストールされたSSON	**新しいReceiverインストールの間のSSONオプション** **（コマンドライン - /includeSSONまたはUIオプションをチェック）**	**動作**
はい	はい	SSONコンポーネントがアップグレードされる レジストリキーが作成される SSON機能が実行される – 有効にするために必要な操作はありません
はい	いいえ	SSONコンポーネントがアップグレードされる レジストリキーが作成される SSON機能の実行 – 有効にするために必要な操作はありません
いいえ	はい	SSONコンポーネントがアップグレードされる レジストリキーが作成される SSON機能の無効化 – ユーザーはReceiverをアインインストールし、コマンドラインオプションの/includeSSONを介して、またはGUIオプションによりSSONを有効にして再インストールする必要があります
いいえ	いいえ	SSONコンポーネントはインストールされません

注：シングルサインオンの有効化インストールウィザードは、既存のバージョンのCitrix Receiverをアップグレードする場合は使用できません。

Receiver for Windowsの削除

コントロールパネルの［プログラムと機能］（または［プログラムの追加と削除］）を使ってReceiverをアンインストールできます。

コマンドラインを使ってReceiverをアンインストールするには

ユーザーは、コマンドラインから以下のコマンドを実行してReceiverをアンインストールすることもできます。

CitrixReceiver.exe /uninstall

ユーザーデバイスからReceiverをアンインストールした後、Receiver.adm/Receiver.admlまたはReceiver.admxにより作成されたReceiverのカスタム設定レジストリキーが、HKEY_LOCAL_MACHINEおよびHKEY_LOCAL_USERの下のSoftware\Policies\Citrix\ICA Clientディレクトリに残ります。 Receiverを再インストールする場合、これらのポリシーによって予期せぬ問題が発生することがあります。 これらカスタムポリシーは、手作業で削除してください。

> **警告**
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール

Aug 30, 2016

コマンドラインオプションを指定して、Citrix Receiverのインストーラーをカスタマイズします。 セットアッププログラムが起動する前にインストーラーパッケージはユーザーの一時フォルダーに自己展開され、%temp%フォルダーにはおおよそ57.8 MBの空き領域が必要です。 領域要件には、プログラムファイル、ユーザーデータ、およびいくつかのアプリケーションを起動した後の一時ディレクトリが含まれます。

> **警告**
>
> レジストリエディタの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

コマンドプロンプトからCitrix Receiver for Windowsをインストールするには、次の構文を使用します：

CitrixReceiver.exe []

使用方法情報の表示

オプション	/? または/help
説明	この切り替えにより使用方法情報が表示されます。
使用サンプル	CitrixReceiver.exe /? CitrixReceiver.exe /help

UIインストール時の再起動の抑制

オプション	/noreboot
説明	UIインストール時に再起動を抑制します。 サイレントインストールを行う場合、このオプションを指定する必要ありません。 再起動されないようにする場合、Receiverのインストール時に一時停止状態だったUSBデバイスは、ユーザーデバイスを再起動するまでReceiverで認識できません。
使用サンプル	CitrixReceiver.exe /noreboot

サイレントインストール

オプション	/silent
説明	エラーメッセージや進行状況を示すダイアログボックスが開かなくなり、完全なサイレントインストールを実行できます。
使用サンプル	CitrixReceiver.exe /silent

認証時のシングルサインオンの有効化

オプション	/includeSSON
説明	シングルサインオン認証（パススルー認証）がインストールされます。 スマートカードでシングルサインオンする場合は、このオプションを指定する必要があります。 コマンドラインで/includeSSONを指定すると、関連のオプションENABLE_SSONが有効になります。 ADDLOCAL=で機能を指定してシングルサインオン機能をインストールする場合は、値としてENABLE_SSONも指定する必要があります。 ユーザーデバイスに対してパススルー認証を有効にするには、/includeSSONオプションを指定したコマンドラインからローカルの管理者権限でReceiverをインストールする必要があります。 またユーザーデバイスで、［管理者テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrixコンポーネント］、［Citrix Receiver］、［ユーザー認証］の順に選択して、これらのポリシーを有効にする必要もあります。 ● ローカルユーザー名とパスワード ● パススルー認証の有効化 ● すべてのICAに対してパススルー認証を有効にします（Web Interface構成およびセキュリティ設定により必要／不必要が異なる）。 変更が完了したら、ユーザーデバイスを再起動します。 詳しくは、『How to Manually Install and Configure Citrix Receiver for Pass-Through Authentication」を参照してください。 注：スマートカード、Kerberosとローカルユーザー名、およびパスワードポリシーは相互依存しています。構成順序が重要です。 最初に必要にないポリシーを無効にしてから、次に必要なポリシーを有効にすることをお勧めします。 その結果について慎重に検証してください。
使用サンプル	CitrixReceiver.exe /includeSSON

/includeSSONの指定時にシングルサインオンを有効化

オプション	ENABLE_SSON={Yes | No}

説明	/includeSSONの指定時にシングルサインオンを有効にします。 デフォルト値はYesです。 さらに/includeSSONを指定すると、シングルサインオンが有効になります。 スマートカードによるシングルサインオンを有効にするには、このプロパティを指定する必要があります。 有効にしたシングルサインオン認証は、インストール後にユーザーがデバイスにログオンし直すまで使用できません。 管理者権限が必要です。
使用サンプル	CitrixReceiver.exe /ENABLE_SSON=Yes

常時トレース

オプション	/EnableTracing={true | false}
説明	この機能はデフォルトで有効になっています。 このプロパティを使用して、常時トレース機能を明示的に有効化または無効化します。 常時トレースは、接続時間に関する重大なログの収集に役立ちます。 これらのログは断続的な接続の問題のトラブルシューティングに役立つことがあります。 常時トレースポリシーによりこの設定は上書きされます。 デフォルトでは、常時トレースログ ファイルは、*C:\Users\\AppData\Local\Temp\CTXReceiverLogs\\xxx.etl*ディレクトリにあります。
使用サンプル	CitrixReceiver.exe /EnableTracing=true

カスタマーエクスペリエンス向上プログラム（CEIP）の使用

オプション	/EnableCEIP={true | false}
説明	Citrixのカスタマーエクスペリエンス向上プログラム（CEIP）への参加を有効にすると、匿名の統計および使用状況情報が、Citrix製品の品質およびパフォーマンスを向上させる目的で送信されます。
使用サンプル	CitrixReceiver.exe /EnableCEIP=true

インストールディレクトリの指定

オプション	INSTALLDIR=
	インストールパスを指定します。ここでInstallation Directoryは、ほとんどのCitrix Receiverソフトウェアがインストールされる場所です。 デフォルト値は、C:\Program Files\Citrix\Receiverです。 ただし、Citrix Receiverの一部の

説明	コンポーネント（Authentication Manager、Receiver、およびSelf-Service Plug-in）はC:\Program Files\Citrixにインストールされます。 このオプションでを指定する場合は、\ReceiverディレクトリにRIInstaller.msiをインストールし、ディレクトリにほかのMSIファイルをインストールする必要があります。
使用サンプル	CitrixReceiver.exe INSTALLDIR=c:\Citrix\Test

サーバーファームに対するユーザーデバイスの識別

オプション	CLIENT_NAME=<*ClientName*>
説明	クライアント名を指定します。ここでClientNameは、サーバーファームでユーザーデバイスを識別するために使用される名前です。 デフォルト値は、%COMPUTERNAME%です。
使用サンプル	CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%.

ダイナミッククライアント名

オプション	ENABLE_CLIENT_NAME=Yes | No
説明	ダイナミッククライアント名機能を有効にすると、コンピューター名がクライアント名として使用されます。 この場合、ユーザーがコンピューター名を変更すると、クライアント名もそれに応じて変更されます。 デフォルトはYesです。 ダイナミッククライアント名機能を無効にするには、このプロパティをNoに設定し、CLIENT_NAMEプロパティの値を指定します。
使用サンプル	CitrixReceiver.exe DYNAMIC_NAME=Yes

指定したコンポーネントのインストール

オプション	ADDLOCAL=
	1つまたは複数の指定したコンポーネントをインストールします。 複数のパラメーターを指定する場合は、以下の各パラメーターをスペースなしのコンマで区切ります。 大文字と小文字は区別されます。 このキーを指定しない場合、すべてのコンポーネントがデフォルトでインストールされます。 注：ReceiverInsideとICA_Clientは必須であり、ほかのコンポーネントをインストールする場合でも必ずこれらを含める必要があります。

説明	注：ADDLOCALが指定されていない場合、SSON以外のデフォルトのコンポーネントがすべてインストールされます。 次のコンポーネントがあります。 • ReceiverInside – Citrix Receiverエクスペリエンスをインストールします（Receiverの操作に必要なコンポーネント）。 • ICA_Client – 標準のCitrix Receiverをインストールします（Receiverの操作に必要なコンポーネント）。 • WebHelper – WebHelperコンポーネントをインストールします。このコンポーネントはICAファイルをStorefrontから取得してHDXエンジンに渡します。 さらに、環境パラメーターを検証しStorefrontと共有します。これはICOクライアント検出と同様です。 • SSON – シングルサインオン（パススルー認証）機能をインストールします。 管理者権限が必要です。 • AM – Authentication Managerをインストールします。 • SELFSERVICE – Self-service Plug-inをインストールします。 AM値はコマンドラインで指定し、ユーザーデバイスにNET 3.5 Service Pack 1をインストールする必要があります。 Self-Service Plug-inは、.NET 3.5をサポートしないWindows Thin PCデバイスでは使用できません。 • Self-Service Plug-in（SSP）のスクリプト、およびReceiver for Windows 4.2以降で使用できるパラメーターについて詳しくは、 http://support.citrix.com/article/CTX200337を参照してください。 • このセクションの「仮想デスクトップやアプリケーションをコマンドラインで起動するには」で説明されているように、ユーザーはSelf-Service Plug-inを使ってReceiverのウインドウまたはコマンドラインから仮想デスクトップやアプリケーションにアクセスできます。 • USB – USBサポートをインストールします。 管理者権限が必要です。 • DesktopViewer – Desktop Viewerをインストールします。 • Flash – HDX MediaStream for Flashをインストールします。 • Vd3d – Windows Aeroエクスペリエンスを有効にします（Aeroをサポートするオペレーティングシステムが対象です）。
使用サンプル	CitrixReceiver.exe ADDLOCAL=ReceiverInside、ICA_Client、SSON

Merchandising Serverの配信を介して構成されなかったストアの構成

オプション	ALLOWADDSTORE={N | S | A}
	Merchandising Serverの配信により構成されなかったストアをユーザーが追加および削除できるかどうかを指定します。ユーザーは、Merchandising Serverの配信により構成されたストアを有効または無効にできますが、そのようなストアを削除したり、名前やURLを変更したりすることはできません。デフォルトはSです。 次のオプションがあります。 • N – ユーザーによるストアの追加や削除を許可しません。 • S – ユーザーによるストアの追加や削除を許可します（HTTPSで構成されたセキュアなストアのみ）。 • A – ユーザーによるストアの追加や削除を許可します（HTTPSまたはHTTPで構成されたストア）。 Citrix Receiverをユーザー単位でインストールする場合には適用されません。 この機能は、レジストリキーHKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore

説明	で設定することもできます。 注：デフォルトでは、HTTPSによるセキュアなストアのみが許可されます。実稼働環境では、このデフォルト設定の使用をお勧めします。 テスト環境でHTTPストア接続を使用するには、以下の構成を行います。 1. HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStoreにAを設定すると、HTTPによる非セキュアなストアをユーザーが追加できるようになります。 2. HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwdにAを設定すると、非セキュアなストアでユーザーがパスワードを保存できるようになります。 3. StoreFrontで構成された［TransportType］が［HTTP］のストアを追加するには、HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\AuthManagerに値ConnectionSecurityMode（REG_SZ）を追加して、Anyを設定します。 4. Citrix Receiverの終了と再起動
使用サンプル	CitrixReceiver.exe ALLOWADDSTORE=N

PNAgentプロトコルを使ったストアの資格情報のローカルでの保存

オプション	ALLOWSAVEPWD={N | S | A}
説明	Merchandising Serverの配信により構成されなかったストアをユーザーが追加および削除できるかどうかを指定します。ユーザーは、Merchandising Serverの配信により構成されたストアを有効または無効にできますが、そのようなストアを削除したり、名前やURLを変更したりすることはできません。デフォルトはSです。 次のオプションがあります。 ● N – ユーザーによるパスワードの保存を許可しません。 ● S – ユーザーによるパスワードの保存を許可します（HTTPSで構成されたセキュアなストアのみ）。 ● A – ユーザーによるパスワードの保存を許可します（HTTPSまたはHTTPで構成されたストア）。 この機能は、レジストリキーHKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwdで設定することもできます。 注：AllowSavePwdが機能しない場合は、次のレジストリーキーを手動で追加する必要があります。 ● 32ビットOSクライアントのキー：HKLM\Software\Citrix\AuthManager ● 64ビットOSクライアントのキー：HKLM\Software\wow6432node\Citrix\AuthManager ● 種類：REG_SZ ● 値：never – ユーザーによるパスワードの保存を許可しません。 secureonly – ユーザーによるパスワードの保存を許可します（HTTPSで構成されたセキュアなストアのみ）。 always – ユーザーによるパスワードの保存を許可します（HTTPSまたはHTTPで構成されたストア）。
使用サンプル	CitrixReceiver.exe ALLOWSAVEPWD=N

Select certificate

オプション	AM_CERTIFICATESELECTIONMODE={Prompt | SmartCardDefault | LatestExpiry}
説明	このオプションを使って証明書を選択します。デフォルト値はPromptで、ユーザーが証明書を選択するための一覧が表示されます。 デフォルトの証明書（スマートカードプロバイダー指定の証明書）が使用されるようにしたり、長い有効期限が残っているものが使用されるようにしたりできます。 有効なログオン証明書がない場合はユーザーにメッセージが表示され、使用可能なほかのログオン方法が提示されます。 この機能は、レジストリキーHKEY_CURRENT_USERまたはHKEY_LOCAL_MACHINEのSoftware\[Wow6432Node\]Citrix\AuthManagerのCertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }で設定することもできます。 最適な証明書をユーザーが選択できるように、HKEY_CURRENT_USERでの設定は、HKEY_LOCAL_MACHINEの設定よりも優先されます。
使用サンプル	CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt

CSPコンポーネントを使ったスマートカードPINエントリの管理

オプション	AM_SMARTCARDPINENTRY=CSP
説明	CSPコンポーネントを使ってスマートカードPINエントリを管理します。 デフォルトでは、スマートカードのCryptographic Service Provider（CSP）ではなくCitrix ReceiverによりPIN入力用のメッセージが表示されます。 PINの入力が必要な場合、Receiverがメッセージを表示して、ユーザーにより入力されたPINをスマートカードのCSPに渡します。 このプロパティを設定すると、CSPコンポーネントによりPIN入力用のメッセージが表示され、PINが処理されます。
使用サンプル	CitrixReceiver.exe AM_SMARTCARDPINENTRY=CSP

Kerberosの使用

オプション	ENABLE_KERBEROS={Yes | No}
説明	デフォルト値はNoです。 HDXエンジンでKerberos認証を使用するかどうかを指定します。シングルサインオン（パススルー）認証が有効な場合のみ適用されます。 詳しくは、「Kerberosを使用したドメインパススルー認証の構成」を参照してください。
使用	

サンプル	CitrixReceiver.exe ENABLE_KERBEROS=No

レガシFTAアイコンの表示

オプション	LEGACYFTAICONS={False | True}
説明	レガシFTAアイコンを表示するにはこのオプションを使用します。 デフォルト値は、Falseです。 サブスクライブするアプリケーションに関連付けられているファイルタイプのドキュメントに、そのアプリケーションアイコンを表示するかどうかを指定します。 この引数をFalseに設定すると、特定のアイコンが関連付けられていないドキュメントにWindowsによるアイコンが表示されます。 Windowsによるアイコンは、汎用のドキュメントアイコン上にアプリケーションの小さいアイコンが重なって表示されます。 Windows 7を使用するユーザーにMicrosoft Officeアプリケーションを配信する場合は、このオプションを有効にすることをお勧めします。
使用サンプル	CitrixReceiver.exe LEGACYFTAICONS=False

事前起動の有効化

オプション	ENABLEPRELAUNCH={False | True}
説明	デフォルト値は、Falseです。 セッションの事前起動については、「アプリケーションの起動時間の短縮」を参照してください。
使用サンプル	CitrixReceiver.exe ENABLEPRELAUNCH=False

［スタート］メニューショートカット用ディレクトリの指定

オプション	STARTMENUDIR={Directory Name}
	デフォルトでは、［スタート］>［すべてのプログラム］の下にアプリケーションのショートカットが追加されます。 ユーザーがサブスクライブしたアプリケーションのショートカットを配置するフォルダーを［すべてのプログラム］からの相対パスで指定します。 たとえば、［スタート］>［すべてのプログラム］>［Receiver］にショートカットを配置するには、STARTMENUDIR=\Receiver\と指定します。 ユーザーは、必要に応じてこのフォルダー名を変更したりフォルダーを移動したりできます。 以下のレジストリキーを使用してこの機能を制御することもできます。StartMenuDirにREG_SZ値を作成して、値のデータとして「\RelativePath c 」を入力します。 場所： HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle

説明	HKEY_CURRENT_USER\Software\Citrix\Dazzle XenAppで［クライアントアプリケーションフォルダー］（「Program Neighborhoodフォルダー」とも呼ばれます)を指定して公開されたアプリケーションでは、ショートカットの配置先パスにそのフォルダー名が追加されるように設定できます。これを行うには、UseCategoryAsStartMenuPathにREG_SZ値を作成して、値のデータとして「true」を入力します。 レジストリの場所は上記と同じです。 注：Windows 8/8.1では、［スタート］メニュー内には階層分けされたフォルダーを作成できません。 アプリケーションは個々に、またはXexAppで定義されたカテゴリサブフォルダー内ではないルートフォルダーの下に表示されます。 例 • ［クライアントアプリケーションフォルダー］に「\Office」が設定されているアプリケーションでは、UseCategoryAsStartMenuPathにtrueを設定してStartMenuDirを指定しない場合、［スタート］>［すべてのプログラム］>［Office］にショートカットが配置されます。 • また、［クライアントアプリケーションフォルダー］が「\Office」で、UseCategoryAsStartMenuPathにtrueを設定してStartMenuDirに\Receiverを指定する場合、［スタート］>［すべてのプログラム］>［Receiver］>［Office］にショートカットが配置されます。 これらの設定を変更しても、配置済みのショートカットには反映されません。 ショートカットに設定を反映させるには、そのアプリケーションをアンインストールしてから再インストールする必要があります。
使用サンプル	CitrixReceiver.exe STARTMENUDIR=\Office

ストア名の指定

オプション	STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On | Off];[storedescription]" [STOREy="..."]
説明	このオプションを使ってストア名を指定します。 Citrix Receiverで使用するストアを10まで指定します。 値のデータ： • xおよびy – 0～9の整数。 • storename – デフォルト値はstore。 これは、StoreFrontサーバーで構成される名前と同じである必要があります。 • servername.domain – ストアをホストするサーバーの完全修飾ドメイン名。 • IISLocation – IIS内のストアへのパス。 このストアURLは、StoreFrontプロビジョニングファイルに記述されているURLと同じである必要があります。 ストアURLは、「/Citrix/store/discovery」の形式で指定します。 URLを取得するには、StoreFrontからプロビジョニングファイルをエクスポートしてそれをメモ帳などのテキストエディターで開き、エレメントからURLをコピーします。 • On | Off – Offを指定すると、無効なストアを配信できるようになります。これにより、そのストアにアクセスするかどうかをユーザーが選択できるようになります。 このオプションを指定しない場合、デフォルトの設定はOnになります。 • storedescription – ストアの説明（任意。「HR App Store」など）。 注：このリリースでは、パススルー認証が正しく実行されるように、ストアURLに「/discovery」を追加してく

	ださい。
使用サンプル	CitrixReceiver.exe STORE0="Store;https://test.xx.com/Citrix/Store/Discovery"

ユーザーデバイスでのURLリダイレクトの有効化

オプション	ALLOW_CLIENTHOSTEDAPPSURL=1
説明	ユーザーデバイスのURLリダイレクト機能を有効にします。 管理者権限が必要です。 また、Citrix Receiverをすべてのユーザー用にインストールする必要があります。 URLリダイレクトについては、XenDesktop 7のドキュメントの「ローカルアプリケーションアクセス」のセクションを参照してください。
使用サンプル	CitrixReceiver.exe ALLOW_CLIENTHOSTEDAPPSURL=1

セルフサービスモードの有効化

オプション	SELFSERVICEMODE={False | True}
説明	デフォルト値は、Trueです。 管理者がSelfServiceModeフラグをfalseに設定すると、ユーザーはセルフサービスのCitrix Receiverユーザーインターフェイスにアクセスできなくなります。 その代わりに［スタート］メニューから、および「ショートカットのみのモード」というデスクトップショートカットを介して、サブスクライブされたアプリケーションにアクセスできます。
使用サンプル	CitrixReceiver.exe SELFSERVICEMODE=False

デスクトップショートカット用ディレクトリの指定

オプション	DESKTOPDIR=
説明	すべてのショートカットを単一のフォルダーにまとめます。 デスクトップショートカットのためCategoryPathがサポートされます。 注：DESKTOPDIRオプションを使用する場合、PutShortcutsOnDesktopキーをTrueに設定します。
使用サンプル	CitrixReceiver.exe DESKTOPDIR=\Office

サポートされていないCitrix Receiverバージョンからのアップグレード

オプション	/rcu
説明	サポートされていないバージョンを最新バージョンのCitrix Receiverにアップグレードできます。
使用サンプル	CitrixReceiver.exe /rcu

無人インストール時におけるインストール完了のメッセージの表示

インストールが完了したら、インストールに成功したことを示すダイアログボックスが表示され、**[アカウントの追加]** 画面が開きます。 初めて使用するユーザーは、［アカウントの追加］ダイアログボックスにメールまたはサーバーアドレスを入力してアカウントをセットアップする必要があります。

> **注意**
>
> 前述のSTOREx引数により、またはグループポリシーオブジェクトにより共通ストアが定義されていなかった場合、Citrix Receiverがインストールされているコンピューターにログオンしていなかったユーザーには［アカウントの追加］ダイアログボックスが開きます。 このダイアログボックスが開かないようにするには、キー HKLM\Software\Citrix\ReceiverにREG_DWORD値の EnableX1FTU を作成し、値を0に設定します。

インストールのトラブルシューティング

インストールで問題が発生した場合は、ユーザーの%TEMP%/CTXReceiverInstallLogsディレクトリに生成されるログファイルを確認してください。これらのログファイルの名前は、以下のように「CtxInstall-」または「TrolleyExpress- 」で始まります。 次に例を示します。

CtxInstall-ICAWebWrapper-20141114-134516.log

TrolleyExpress-20090807-123456.log

コマンドラインを使用したインストールの例

以下のコマンドでは、すべてのコンポーネントをサイレントインストールして2つのアプリケーションストアを指定します。

```
CitrixReceiver.exe /silent STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR App Store"
STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/discovery;on;Backup HR App Store"
```

以下のコマンドでは、シングルサインオン（パススルー認証）を指定して、XenApp ServicesサイトのURLを定義したストアを追加します。

```
CitrixReceiver.exe /INCLUDESSON /STORE0="PNAgent;https://testserver.net/Citrix/PNAgent/config.xml;on;My PNAgent Site"
```

仮想デスクトップやアプリケーションをコマンドラインで起動するには

Citrix Receiverにより、サブスクライブ済みの各デスクトップやアプリケーションについてスタブアプリケーションが作成されます。 このアプリケーションを使用して、デスクトップやアプリケーションをコマンドラインから起動できます。 スタブ

アプリケーションは、%appdata%\Citrix\SelfServiceに作成されます。 スタブアプリケーションの名前には、元のアプリケーションの表示名からスペースが削除されたものが設定されます。 たとえば、Internet Explorerのスタブアプリケーション名は、「InternetExplorer.exe」です。

Active Directoryとサンプルのスタートアップスクリプトを使用したReceiver for Windowsの展開

Feb 02, 2016

Active Directoryのグループポリシースクリプトを使用して、Active Directoryの組織構造に基づいてシステムにReceiverを事前に展開することができます。 .msiファイルを抽出するよりもスクリプトを使用することをお奨めします。スクリプトで展開すれば、インストール、アップグレード、およびインストールを1か所から実行し、［プログラムと機能］に表示されるCitrixエントリを統合し、展開済みのReceiverのバージョンを簡単に検出することができます。 グループポリシー管理コンソール（GPMC）の［コンピューターの構成］または［ユーザーの構成］で、［スクリプト］設定を使用します。 スタートアップスクリプトの概要については、Microsoft社のドキュメントを参照してください。

CitrixReceiver.exeのインストールとアンインストールを実行する、サンプルのコンピューター単位のスタートアップスクリプトが収録されています。 スクリプトは、新しいバージョンのXenAppおよびXenDesktopのインストールメディアのCitrix Receiver and Plug-ins\Windows\Receiver\Startup_Logon_Scriptsフォルダーに収録されています。

- CheckAndDeployReceiverPerMachineStartupScript.bat
- CheckAndRemoveReceiverPerMachineStartupScript.bat

Active Directoryのグループポリシーを使用してコンピューターの起動時またはシャットダウン時にスクリプトを実行する場合、カスタム構成ファイルがシステムの既定のユーザープロファイルに作成されることがあります。 これらの構成ファイルにより、一部のユーザーがReceiverのログディレクトリにアクセスできなくなる場合があります。 Citrixのサンプルスクリプトには、これらの構成ファイルを正しく削除するための機能が含まれています。

スタートアップスクリプトを使用してActive DirectoryでReceiverを展開するには

1. 各スクリプトの組織単位を作成します。
2. 新しく作成した組織単位のグループポリシーオブジェクトを作成します。

サンプルスクリプトを変更するには

各ファイルのヘッダーセクションにある次のパラメーターを編集して、スクリプトを変更します。

- **CURRENT VERSION OF PACKAGE（パッケージの現在のバージョン）**： ここに指定するバージョン番号が検証され、そのバージョンが存在しない場合は展開（インストール）が開始されます。 たとえば、 set DesiredVersion= 3.3.0.<XXXX> に、展開するバージョンの番号を指定します。 「3.3.0」などバージョン番号の一部を指定すると、その番号で始まるすべてのバージョン（「3.3.0.1111」や「3.3.0.7777」など）に一致します。
- **PACKAGE LOCATION/DEPLOYMENT DIRECTORY（パッケージの場所/展開ディレクトリ）**： パッケージを格納するネットワーク共有を指定します。この共有にアクセスするための認証はスクリプトで実行しません。 共有フォルダーにEveryoneの読み取りアクセス許可を設定する必要があります。
- **SCRIPT LOGGING DIRECTORY（スクリプトのログディレクトリ）**： インストールログをコピーするネットワーク共有を指定します。この共有にアクセスするための認証はスクリプトで実行しません。 共有フォルダーにEveryoneの読み取り/書き込みアクセス許可を設定する必要があります。
- **PACKAGE INSTALLER COMMAND LINE OPTIONS（パッケージインストーラーのコマンドラインオプション）**： インストーラーに渡すコマンドラインオプションを指定します。 コマンドライン構文については、「コマンドラインパラメーターを使用したCitrix Receiver for Windowsの構成とインストール」を参照してください。

コンピューター単位のスタートアップスクリプトを追加するには

1. グループポリシー管理コンソールを開きます。

2. ［コンピューターの構成］、［ポリシー］、［Windowsの設定］、［スクリプト（スタートアップ/シャットダウン）］の順に選択します。
3. グループポリシー管理コンソールの右ペインで［スタートアップ］を選択します。
4. ［スタートアップのプロパティ］ダイアログボックスで［ファイルの表示］をクリックし、表示されるフォルダーに適切なスクリプトをコピーしてウィンドウを閉じます。
5. ［スタートアップのプロパティ］ダイアログボックスで［追加］をクリックし、［参照］をクリックして新しく作成したスクリプトを検索し追加します。

Receiverをコンピューター単位で展開するには

1. 作成した組織単位に展開対象のユーザーデバイスを移動します。
2. ユーザーデバイスを再起動して任意のユーザーでログオンします。
3. ［プログラムと機能］（以前のオペレーティングシステムでは［プログラムの追加と削除］）に、新しくインストールしたパッケージが表示されていることを確認します。

Receiverをコンピューター単位で削除するには

1. 作成した組織単位に削除対象のユーザーデバイスを移動します。
2. ユーザーデバイスを再起動して任意のユーザーでログオンします。
3. ［プログラムと機能］（以前のオペレーティングシステムでは［プログラムの追加と削除］）から、以前にインストールしたパッケージが削除されていることを確認します。

サンプルのユーザー単位のスタートアップスクリプトの使用

通常、サーバー単位のスタートアップスクリプトを使用することをお勧めします。ただし、Receiverをユーザーごとに構成する必要がある場合は、ユーザー単位のスタートアップスクリプトを使用できます。XenDesktopおよびXenAppのメディアのCitrix Receiver and Plug-ins\Windows\Receiver\Startup_Logon_Scriptsフォルダーには、2つのユーザー単位のスタートアップスクリプトが収録されています。

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

ユーザー単位のスタートアップスクリプトを設定するには

1. グループポリシー管理コンソールを開きます。
2. ［ユーザーの構成］、［ポリシー］、［Windowsの設定］、［スクリプト］の順に選択します。
3. グループポリシー管理コンソールの右ペインで［ログオン］を選択します。
4. ［ログオンのプロパティ］ダイアログボックスで［ファイルの表示］をクリックし、表示されるフォルダーに適切なスクリプトをコピーしてウィンドウを閉じます。
5. ［ログオンのプロパティ］ダイアログボックスで［追加］をクリックし、［参照］をクリックして新しく作成したスクリプトを検索し追加します。

Receiverをユーザー単位で展開するには

1. 作成した組織単位に展開対象のユーザーを移動します。
2. ユーザーデバイスを再起動して特定のユーザーでログオンします。
3. ［プログラムと機能］（以前のオペレーティングシステムでは［プログラムの追加と削除］）に、新しくインストールしたパッケージが表示されていることを確認します。

Receiverをユーザー単位で削除するには

1. 作成した組織単位に削除対象のユーザーを移動します。
2. ユーザーデバイスを再起動して特定のユーザーでログオンします。
3. ［プログラムと機能］（以前のオペレーティングシステムでは［プログラムの追加と削除］）から、以前にインストールしたパッケージが削除されていることを確認します。

Receiver for WebサイトからのReceiver for Windowsの配布

Feb 02, 2016

ReceiverをReceiver for Webサイトからユーザーに配布すると、Webブラウザーからアプリケーションにアクセスするユーザーに確実にReceiverをインストールさせることができます。 Receiver for Webサイトを使用すると、ユーザーはWebページを経由してStoreFrontストアにアクセスできます。 Receiver for Webサイトで適切なバージョンのReceiverがインストールされていないことが検出されると、Receiverをダウンロードしてインストールするためのページが表示されます。 詳しくは、StoreFrontのドキュメントの「Receiver for Webサイト」を参照してください。

Receiver for Webからインストールしたreceiverでは、メールアドレスによるアカウント検出機能を使用できません。 メールアドレスによるアカウント検出機能が構成された環境では、初めて使用するユーザーがReceiverをCitrix.comからインストールすると、メールアドレスまたはサーバーのアドレスの入力が求められます。 ここでユーザーがメールアドレスを入力すると、メールアドレスを使ってアカウントを追加できないという内容のエラーメッセージが表示されます。ユーザーの混乱を避けるため、サーバーアドレスの入力のみが求められるようにします。

1. CitrixReceiver.exeをローカルコンピューターにダウンロードします。
2. CitrixReceiver.exeをCitrixReceiverWeb.exeと名称変更します。
   重要：CitrixReceiverWeb.exeの大文字と小文字は区別されます。
3. 名前を変更した実行可能ファイルを通常の方法で展開します。 StoreFrontを使用している場合は、StoreFrontのドキュメントの「構成ファイルによるReceiver for Webサイトの構成」を参照してください。

Web InterfaceのログオンからのReceiver for Windowsの配布

Feb 02, 2016

この機能は、Web InterfaceをサポートしているXenDesktopおよびXenAppリリースでのみ使用できます。

Web Interfaceのログオン画面でReceiverをユーザーに配布すると、ユーザーがWeb Interfaceを使用する前に確実にReceiverをインストールできます。 Web Interfaceでは、Citrixクライアントソフトウェアを検出して必要に応じてインストールするための機能が提供されます。この機能により、ユーザーは自分の環境に適したソフトウェアをインストールできます。

管理者は、ユーザーがXenApp Webサイトにアクセスしたときに自動的にクライアント検出および展開処理が実行されるように構成できます。 Web Interfaceで適切なバージョンのReceiverがインストールされていないことが検出されると、Receiverをダウンロードしてインストールするためのページが表示されます。

詳しくは、Web Interfaceのドキュメントの「クライアント展開の構成」を参照してください。

Web InterfaceからインストールしたReceiverでは、メールアドレスによるアカウント検出機能を使用できません。 メールアドレスによるアカウント検出機能が構成された環境では、初めて使用するユーザーがReceiverをCitrix.comからインストールすると、メールアドレスまたはサーバーのアドレスの入力が求められます。 ここでユーザーがメールアドレスを入力すると、メールアドレスを使ってアカウントを追加できないという内容のエラーメッセージが表示されます。ユーザーの混乱を避けるため、サーバーアドレスの入力のみが求められるようにします。

1. CitrixReceiver.exeをローカルコンピューターにダウンロードします。
2. CitrixReceiver.exeをCitrixReceiverWeb.exeと名称変更します。
   重要：CitrixReceiverWeb.exeの大文字と小文字は区別されます。
3. XenApp Webサイトの構成ファイル内のClientIcaWin32パラメーターに、変更したファイル名を指定します。
   この機能を使用するには、Web Interfaceサーバー上にReceiverのインストールファイルを配置しておく必要があります。
   Web Interfaceのデフォルトでは、XenAppまたはXenDesktopのインストールメディアで提供されている名前でReceiverのインストールファイルが検索されます。
4. ユーザーは、CitrixReceiverWeb.exeファイルのダウンロードサイトを信頼済みサイトの一覧に追加しておく必要があります。
5. 名前を変更した実行可能ファイルを通常の方法で展開します。

Citrix Receiver for Windowsの構成

Aug 30, 2016

Receiver for Windowsソフトウェアを使用する場合、ホストされているアプリケーションやデスクトップにユーザーがアクセスできるようにするには、以下の構成を行う必要があります。

- アプリケーション配信の構成およびXenDesktop環境の構成。 XenApp環境が正しく構成されていることを確認します。 オプションについて理解し、ユーザーに対しわかりやすいアプリケーションについての説明を提供します。
- StoreFrontアカウントをReceiverに追加して、セルフサービスモードを構成します。 このモードでは、ユーザーがReceiverのユーザーインターフェイスからアプリケーションをサブスクライブできます。
- ショートカットのみのモードを構成します。これには以下の方法が含まれます。
  - グループポリシーオブジェクトテンプレートを使ったショートカットの構成
  - ショートカットカスタマイズ用のレジストリキー。
  - StoreFrontアカウント設定をベースにしたショートカットの構成
- ユーザーにアカウント情報を提供します。 ユーザーがアカウントをセットアップするための情報を提供します。ユーザーは、このアカウントを使用して仮想デスクトップやアプリケーションにアクセスします。 環境によっては、ユーザーが手作業でアカウントをセットアップする必要があります。

- 外部から接続するユーザー（遠隔地からまたはインターネット経由で接続するユーザーなど）にアクセスを提供するには、NetScaler Gatewayを使用した認証を構成します。 詳しくは、「Netscaler Gateway」を参照してください。

アプリケーション配信の構成

XenDesktopまたはXenAppでアプリケーションをユーザーに配信するときは、ストアのアプリケーションにアクセスするユーザーのエクスペリエンスを向上させるために、次のオプションについて検討します。

Webアクセスモード

いずれの構成を実行することなく、Citrix Receiver for Windowsではアプリケーションやデスクトップに対するブラウザーベースのアクセスであるWebアクセスを実行できます。 Receiver for WebまたはWeb Interfaceサイトをwebブラウザーで開き、使用するアプリケーションを選択して実行するだけです。 Webアクセスモードでは、ユーザーのデバイスのアプリケーションフォルダーにアプリケーションのショートカットが置かれます。

セルフサービスモード

StoreFrontまたはWeb Interface Servicesサイトのアカウントを Receiver for Windowsに追加することにより、セルフサービスモードを構成できます。これにより、ユーザーはReceiverを介してアプリケーションをサブスクライブできます。 この拡張ユーザーエクスペリエンスはモバイルアプリケーションストアのものと同様です。 セルフサービスモードでは、必要に応じて必須設定、自動プロビジョニング設定、お勧めのアプリケーションキーワード設定を構成できます。 いずれかのユーザーがアプリケーションを選択すると、そのアプリケーションに対するショートカットがユーザーデバイスのアプリケーションフォルダーに置かれます。

StoreFront 3.0サイトにアクセスすると、Receiverユーザーエクスペリエンスを体験できます。 Receiverユーザーエクスペリエンスについて詳しくは、「ReceiverおよびStoreFront 3.0 Technology Preview」を参照してください。

XenAppファームでアプリケーションを公開する場合、StoreFrontストアを介したアプリケーションへのユーザーアクセスの利便性を高めるため、公開アプリケーションについてわかりやすい説明を付加してください。 この説明は、Citrix Receiverを介してユーザーに表示できます。

セルフサービスモードの構成

以前にも説明したように、XenAppアカウントをReceiverに追加したり、Web InterfaceのXenApp Servicesサイトをポイントするように Receiverを構成したりして、セルフサービスモードを構成できます。これにより、ユーザーはReceiverのユーザーインターフェイスを介してアプリケーションをサブスクライブできます。 この拡張ユーザーエクスペリエンスはモバイルアプケーションストアのものと同様です。

セルフサービスモードでは、必要に応じて必須設定、自動プロビジョニング設定、お勧めのアプリケーションキーワード設定を構成できます。

- アプリケーションがストアのユーザー全員に自動的にサブスクライブされるようにするには、XenAppでそのアプリケーションを公開するときに、説明にKEYWORDS:Autoという文字列を追加します。 ユーザーがストアにログオンすると、そのアプリケーションを手動でサブスクライブしなくても自動的にプロビジョニングされます。
- 説明にKEYWORDS:Featuredという文字列を追加すると、そのアプリケーションがCitrix Receiverの [おすすめ] 一覧に表示され、ユーザーがそのアプリケーションを見つけやすくなります。

詳しくは、StoreFrontのドキュメントを参照してください。

XenApp展開環境のWeb Interfaceで、XenApp Servicesサイトを作成します。 サイト名およびその作成方法は、インストールしているWeb Interfaceのバージョンにより異なります。 詳しくは、Web Interfaceのドキュメントを参照してください。

> **注意**
>
> セルフサービスモードを使ってセッションを起動する場合、デフォルトで自動接続が有効になっています。

StoreFrontの構成

StoreFrontで作成するストアは、Citrix Receiverのリソース配信インフラストラクチャと認証を提供するサービスにより構成されます。 このストアにより、XenDesktopサイトおよびXenAppファームからデスクトップとアプリケーションが列挙および集約され、これらのリソースをユーザーが使用できるようになります。

1. StoreFrontをインストールして構成します。 詳しくは、StoreFrontのドキュメントを参照してください。

   注：独自のReceiverダウンロードサイトを作成する管理者用に、テンプレートが提供されています。

アプリケーション配信の構成

Oct 31, 2016

XenDesktopやXenAppでアプリケーションをユーザーに配信するときは、ストアのアプリケーションにアクセスするユーザーのエクスペリエンスを向上させるために、次のオプションについて検討します。

- Webアクセスモード - いずれの構成もすることなく、Receiver for Windows 4.4ではアプリケーションおよびデスクトップにブラウザーベースのアクセスが提供されます。 Receiver for WebまたはWeb InterfaceサイトをWebブラウザーで開き、使用するアプリケーションを選択して実行するだけです。 このモードでは、ユーザーのデスクトップにショートカットは置かれません。
- セルフサービスモード - StoreFrontアカウントをReceiverに追加したり、StoreFrontサイトをポイントするようにReceiverを構成したりするだけで、「セルフサービスモード」を構成できます。これにより、ユーザーはReceiverのユーザーインターフェイスを介してアプリケーションをサブスクライブできます。 この拡張ユーザーエクスペリエンスはモバイルアプリケーションストアのものと同様です。セルフサービスモードでは、必要に応じて必須設定、自動プロビジョニング設定、お勧めのアプリケーションキーワード設定を構成できます。

注：デフォルトでは、ユーザーはReceiver for Windows 4.4 を使い、［スタート］メニューに表示するアプリケーションを選択できます。

- アプリケーションショートカットのみのモード - Receiver管理者として、Receiver for Windows 4.4 Enterpriseでするのと同じように、Receiver for Windows 4.4.3.4でアプリケーションやデスクトップのショートカットを［スタート］メニューまたはデスクトップに直接配置するよう構成できます。 新しい「ショートカットのみ」のモードにより、ユーザーはアプリケーションの検索で使い慣れたWindowsのナビゲーションスキーム内で公開アプリケーションを見つけることができます。

XenAppおよびXenDesktop 7を使ったアプリケーション配信については、「デリバリーグループアプリケーションの作成」を参照してください。

注：デリバリーグループのアプリケーションにわかりやすい説明を入力します。 Webアクセスまたはセルフサービスモードを使う場合、Receiverのユーザーにはこの説明が表示されます。
［スタート］メニュー内またはデスクトップ上でショートカットを構成する方法について詳しくは、「ショートカットのみのモードの構成」を参照してください。

セルフサービスモードの構成

StoreFrontアカウントをReceiverに追加したり、StoreFrontサイトをポイントするようにReceiverを構成したりするだけで、「セルフサービスモード」を構成できます。これにより、ユーザーはReceiverのユーザーインターフェイスを介してアプリケーションをサブスクライブできます。 この拡張ユーザーエクスペリエンスはモバイルアプリケーションストアのものと同様です。

注：デフォルトでは、ユーザーはReceiver for Windows 4.4 を使い、［スタート］メニューに表示するアプリケーションを選択できます。セルフサービスモードでは、必要に応じて必須設定、自動プロビジョニング設定、お勧めのアプリケーションキーワード設定を構成できます。

デリバリーグループアプリケーションの説明に、適切なキーワードを追加します。

- 個々のアプリケーションを必須にしてReceiver for Windowsから削除できないようにするには、アプリケーションの説明に「KEYWORDS:Mandatory」という文字列を追加します。 ユーザーが必須アプリケーションをサブスクリプション解除するための削除オプションはありません。
- アプリケーションがストアのユーザー全員に自動的にサブスクライブされるようにするには、説明に「KEYWORDS:Auto」という文字列を追加します。 ユーザーがストアにログオンすると、そのアプリケーションを手動でサブスクライブしなくても自動的にプロビジョニングされます。
- 説明に「KEYWORDS:Featured」という文字列を追加すると、そのアプリケーションがCitrix Receiverの［おすすめ］一覧に表示され、ユーザーがそのアプリケーションを見つけやすくなります。

アプリケーションショートカットの場所のカスタマイズ

［スタート］メニュー統合およびデスクトップショートカットのみのモードにより、公開アプリケーションのショートカットをWindowsの［スタート］メニューやデスクトップ上に配置できます。 この方法では、ユーザーはReceiverのユーザーインターフェイスからアプリケーションをサブスクライブする必要がありません。 これらの機能により、ユーザーのグループにシームレスなデスクトップエクスペリ

エンスを提供して、ユーザーは頻繁に使用するアプリケーションに一貫した方法でアクセスできるようになります。

Receiver管理者として、コマンドラインインストールフラグ、GPO、アカウントサービス、またはレジストリ設定を使って通常の「セルフサービス」Receiverインターフェイスを無効にし、事前定義した［スタート］メニューと置き換えることができます。 このフラグはSelfServiceMode と呼ばれ、デフォルトで true に設定されています。 管理者が SelfServiceMode フラグを falseに設定すると、ユーザーにセルフサービスのReceiverユーザーインターフェイスにアクセスできなくなります。 その代わり、［スタート］メニューやデスクトップのショートカットを使って、サブスクライブ済みのアプリケーションにアクセスします。これを**ショートカットのみのモード**と呼びます。

ユーザーおよび管理者は、いくつかのレジストリ設定を使用してアプリケーションのショートカットをカスタマイズできます。 「アプリケーションショートカットをカスタマイズするためのレジストリキーの使用」を参照してください。

ショートカットの操作

- ユーザーはアプリケーションを削除できません。 すべてのアプリケーションを必須アプリケーションにするには SelfServiceMode フラグを false に設定します（ショートカットのみのモード）。 ユーザーがデスクトップからショートカットアイコンを削除しても、システムトレイのReceiverアイコンで［更新］を選択するとこれらのアイコンが再表示されます。
- ユーザーはストアを1つだけ構成できます。アカウントおよび基本設定オプションは使用できません。 このため、ユーザーが追加のストアを構成できません。 管理者はユーザーに特別な権限を付与し、これによりユーザーはグループポリシーオブジェクトテンプレートを使用して、またはクライアントマシンでレジストリキー（HideEditStoresDialog）を手動で追加して1つまたは複数のアカウントを追加できます。 管理者がユーザーにこの権限を付与すると、ユーザーのシステムトレイのReceiverアイコンに［基本設定］オプションが表示され、アカウントを追加および削除できるようになります。
- ユーザーはWindowsのコントロールパネルを介してアプリケーションを削除することはできません。
- カスタマイズ可能なレジストリ設定を介してデスクトップショートカットを追加できます。 デスクトップショートカットはデフォルトでは追加できません。 レジストリ設定を変更したら、Receiverを再起動する必要があります。
- ショートカットは［スタート］メニューにデフォルトとしてカテゴリパス UseCategoryAsStartMenuPathとして作成されます。

注：Windows 8/8.1では、［スタート］メニュー内には階層分けされたフォルダーを作成できません。 アプリケーションは個々に、またはXexAppで定義されたカテゴリサブフォルダー内ではないルートフォルダーの下に表示されます。

- インストール時にフラグ [/DESKTOPDIR="Dir_name"] を指定すると、すべてのショートカットを単一のフォルダー内に配置できます。CategoryPath がデスクトップショートカットのためにサポートされます。
- 変更アプリケーションの自動再インストールは、レジストリキー AutoReInstallModifiedAppsを介して有効にできます。AutoReInstallModifiedAppsが有効な場合、管理者がサーバー上の公開アプリケーションおよび公開デスクトップの属性を変更すると、その変更がすべてクライアントマシンに反映されます。 AutoReInstallModifiedAppsが無効な場合、アプリケーションとデスクトップの属性は更新されず、クライアント上で削除されたショートカットも更新時に再格納されません。 デフォルトでは、このAutoReInstallModifiedAppsは有効です。 「アプリケーションショートカットをカスタマイズするためのレジストリキーの使用 を参照してください。

グループポリシーオブジェクトテンプレートを使ったアプリケーションショートカットの場所のカスタマイズ

注：ストアを構成する前にグループポリシーに変更を加える必要があります。 グループポリシーをカスタマイズする場合には管理者かユーザーかに関わらず、Receiverをリセットしてからグループポリシーを構成し、その後でストアを再構成する必要があります。

管理者として、グループポリシーを使ってショートカットを構成できます。

1. 単一のコンピューターにポリシーを適用する場合に［スタート］メニューからgpedit.msc を実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。
2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、Receiver構成フォルダーを参照してからreceiver.admx（またはreceiver.adml）を選択します。 ADMXテンプレートについて詳しくは、「About ADMX Template Usage」を参照してください。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. グループポリシーエディターで、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］、［Self Service］の順に開きます。

7. ［Manage SelfServiceMode］を選択し、セルフサービスモードのReceiverユーザーインターフェイスを有効または無効にします。
8. ［Manage App Shortcut］を選択して、次のことを有効または無効にします。
   - Shortcuts on Desktop
   - Shortcuts in Start menu
   - Desktop Directory
   - Start menu Directory
   - Category path for Shortcuts
   - Remove apps on logoff
   - Remove apps on exit
9. ［Allow users to Add/Remove account］を選択して、1つ以上のアカウントを追加または削除する権限をユーザーに付与します。

アプリケーションショートカットをカスタマイズするためのレジストリキーの使用

> **注意**
>
> デフォルトでは、レジストリキーは文字列形式を使用します。

レジストリキー設定を使ってショートカットをカスタマイズできます。 レジストリキーは次の場所で設定できます。 レジストリキーを適用すると、一覧の優先順でそれが反映されます。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。
注：ストアを構成する前に変更をレジストリキーに入れる必要があります。 レジストリキーをカスタマイズする場合には管理者かユーザーかに関わらず、Receiverをリセットしてからレジストリキーを構成し、その後でストアを再構成する必要があります。
32ビットマシンのレジストリーキー

レジストリー名	デフォルト値	場所の優先順
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
RemoveAppsOnExit	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle

レジストリー名	デフォルト値	場所の優先順
		HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
PutShortcutsInStartMenu	はい	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
SelfServiceMode	はい	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
UseCategoryAsStartMenuPath	はい	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
StartMenuDir	""（空）	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
DesktopDir	""（空）	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle

レジストリー名	デフォルト値	場所の優先順
AutoReinstallModifiedApps	はい	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
HideEditStoresDialog	SelfServiceModeで はTrue、NonSelfServiceModeで はFalse	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
WSCSupported	はい	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
WSCReconnectAll	はい	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	インストール中はレジストリが 作成されません。	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID+\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE \Citrix\Dazzle

64ビットマシンのレジストリーキー

レジストリー名	デフォルト値	場所の優先順
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
RemoveAppsOnExit	False	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
PutShortcutsInStartMenu	はい	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
SelfServiceMode	はい	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
UseCategoryAsStartMenuPath	はい	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle

レジストリー名	デフォルト値	場所の優先順
		HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
StartMenuDir	""（空）	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
DesktopDir	""（空）	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
AutoReinstallModifiedApps	はい	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
HideEditStoresDialog	SelfServiceModeではTrue、NonSelfServiceModeではFalse	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
WSCSupported	はい	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle

レジストリー名	デフォルト値	場所の優先順
WSCReconnectAll	はい	HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectMode	3	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectModeUser	インストール中はレジストリが作成されません。	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID+\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle

アプリケーションショートカットをカスタマイズするためのStoreFrontアカウント設定の使用

［スタート］メニュー内およびデスクトップ上のショートカットをStoreFrontサイトからセットアップできます。C:\inetpub\wwwroot\Citrix\Roamingにあるweb.configファイルのセクションに次の設定を追加できます。

- デスクトップ上にショートカットを置くには、PutShortcutsOnDesktopを使用します。 設定："true"または"false"（デフォルトはfalse）。
- ［スタート］メニュー内にショートカットを置くには、PutShortcutsInStartMenuを使用します。 設定："true"または"false"（デフォルトはtrue）。
- ［スタート］メニュー内のカテゴリパスを使用するには、UseCategoryAsStartMenuPathを使用します。 設定："true"または"false"（デフォルトはtrue）。

注：Windows 8/8.1では、［スタート］メニュー内には階層分けされたフォルダーを作成できません。 アプリケーションは個々に、またはXexAppで定義されたカテゴリサブフォルダー内ではないルートフォルダーの下に表示されます。

- ［スタート］メニュー内のすべてのショートカットを単一のフォルダー内に置くには、StartMenuDirを使用します。 設定：文字列値、ショートカットが書き込まれるフォルダーの名前になります。
- 管理者により変更されたアプリケーションが再インストールされるようにする（変更アプリケーションの自動再インストール機能）には、AutoReinstallModifiedAppsを使用します。 設定："true"または"false"（デフォルトはtrue）。
- デスクトップ上のすべてのショートカットを単一のフォルダー内に置くには、DesktopDirを使用します。 設定：文字列値、ショートカットが書き込まれるフォルダーの名前になります。
- クライアントの'add/remove programs'でエントリを作成しないようにするには、DontCreateAddRemoveEntryを使用します。 設定："true"または"false"（デフォルトはfalse）。
- 以前にはストアーから実行できたけど今はもう実行できないアプリケーションのショートカットやReceiverアイコンを削除するには、SilentlyUninstallRemovedResourcesを使用します。 設定："true"または"false"（デフォルトはfalse）。

web.configファイルで、アカウントのXMLセクションに変更を追加する必要があります。 次の開始タグを検索し、このセクションに移動

します。

このセクションは タグで終わります。
このタグ内にある、次のような最初のプロパティセクションに移動します。

このセクションの タグの後ろにプロパティを追加できます。1行ごとに名前と値を記述します。 次に例を示します。

注： タグの前に追加されたプロパティの要素により、それが無効になることがあります。 プロパティ名と値の追加が任意の場合は、 タグを削除します。
プロパティの追加例：

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。 展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。 変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

XenAppおよびXenDesktop 7.xのアプリケーションごとの設定を使ったアプリケーションショートカットの場所のカスタマイズ

アプリケーションおよびデスクトップショートカットを［スタート］メニュー内に直接またはデスクトップ上に自動的に配置するよう、Receiverを構成できます。 この機能は、以前にリリースされたバージョンのReceiverの機能と似ていますが、バージョン4.4 ではXenAppを使ってアプリケーション設定ごとにアプリケーションショートカットの配置を制御できる機能が導入されています。 この機能は、終始一貫した場所に表示する必要がある一部のアプリケーションが存在する環境で有用です。

ショートカットの場所を指定して、すべてのユーザーが同じ場所でそれにアクセスできるようにするには、XenAppのアプリケーションごとの設定を使用します。

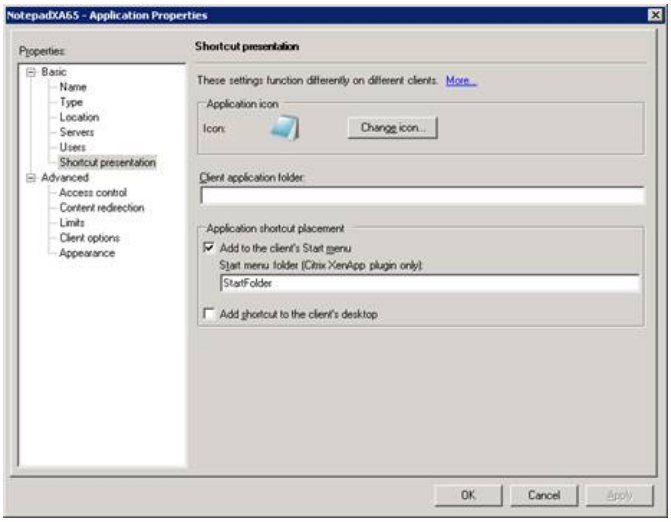
セルフサービスモードになっているかどうかあるいは［スタート］メニューかどうかには関係なく、アプリケーションごとの設定によりアプリケーションを配置する場所を決定する場合は、	Receiverで**PutShortcutsInStartMenu=false**と構成して、アプリケーションごとの設定を有効にします。 注：この設定は、Web Interfaceサイトにのみ適用されます。

注：**PutShortcutsInStartMenu=false**設定は、XenApp 6.5とXenDesktop 7.xの両方に適用されます。

XenApp 6.5でのアプリケーションごとの設定の構成

XenApp 6.5でアプリケーションごとの公開ショートカットを構成するには

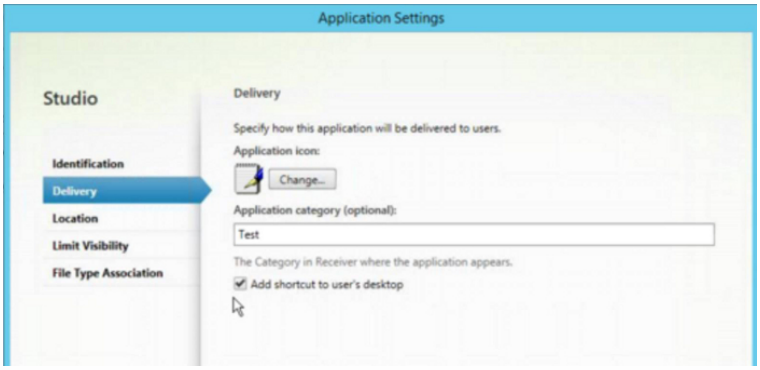
1. XenAppの［アプリケーションのプロパティ］画面で、［基本設定］プロパティを展開します。
2. ［ショートカットの表示］オプションを選択します。
3. ［ショートカットの表示］画面の［アプリケーションのショートカットの追加先］で、［クライアントのスタート メニューに追加する］チェックボックスをオンにします。 チェックボックスをオンにした後、ショートカットを置くフォルダーの名前を入力します。 フォルダー名を指定しない場合は、XenAppにより［スタート］メニューにフォルダーに入っていないショートカットが置かれます。
4. ［ショートカットをクライアントのデスクトップに追加するかどうかを示します]を選択して、クライアントマシンのデスクトップにショートカットを含めます。
5. ［適用］をクリックします。
6. ［OK］をクリックします。



XenAppのアプリケーションごとの設定を使った、アプリケーションショートカットの場所のカスタマイズ

XenApp 7.6でアプリケーションごとの公開ショートカットを構成するには

1. Citrix Studioで、［アプリケーション設定］画面を開きます。
2. ［アプリケーション設定］画面で［配信］を選択します。 この画面を使って、アプリケーションがユーザーにどのように配信されるかを指定できます。
3. アプリケーションの適切なアイコンを選択します。［変更］をクリックして、必要なアイコンの場所を参照します。
4. （オプション）［アプリケーションカテゴリ］に、アプリケーションが表示されるReceiverのカテゴリを指定します。 たとえば、ショートカットをMicrosoft Officeアプリケーションに追加している場合は、「Microsoft Office」と入力します。
5. ［ユーザーのデスクトップにショートカットを追加する］チェックボックスをオンにします。
6. ［OK］をクリックします。



列挙遅延またはアプリケーションスタブデジタル署名の削減

ユーザーのログオン時にアプリケーションの列挙に遅延が生じる場合、またはアプリケーションスタブにデジタル署名が必要な場合、ネットワーク共有から.EXEスタブをcopyする機能がReceiverにより提供されます。

この機能を実行するには、次の複数の手順を実行します。

1. クライアントマシンにアプリケーションスタブを作成します。
2. アプリケーションスタブをネットワーク共有からアクセスできる場所にコピーします。
3. 必要な場合は、ホワイトリストを作成します（または、エンタープライズ証明書でスタブに署名します）。
4. レジストリキーを追加し、ネットワーク共有からスタブをコピーしてReceiverがスタブを作成できるようにします。

RemoveappsOnLogoffおよびRemoveAppsonExitが有効で、ユーザーのログオン時にアプリケーション列挙に遅延が生じる場合、次の解決策により遅延を削減させます。

1. Regeditを使って、HKCU\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"を追加します。
2. Regeditを使って、HKLM\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"を追加します。 HKCUはHKLMよりも優先されます。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。
ネットワーク共有に格納されている事前作成のスタブ実行可能ファイルをマシンが使用できるようにします。

1. クライアントマシン上で、すべてのアプリケーションに対するスタブ実行可能ファイルを作成します。 これを実行するには、Receiver
   を使ってすべてのアプリケーションをマシンに追加します。Receiverは実行可能ファイルを生成します。
2. %APPDATA%\Citrix\SelfServiceからスタブ実行可能ファイルを取得します。 必要なのは.exeファイルだけです。
3. 実行可能ファイルをネットワーク共有にコピーします。
4. ロックダウンされる各クライアントマシンに対して次のレジストリキーを設定します。
   1. Reg add HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\ReceiverStubs"
   2. Reg add HKLM\Software\Citrix\Dazzle /v
   3. CopyStubsFromCommonStubDirectory /t REG_SZ /d "true". また、必要な場合はHKCUでこれらの設定を構成することもできます。 HKCUはHKLMよりも優先されます。
   4. 設定をテストするため、Receiverを終了して再起動します。

ユースケースの例

このトピックでは、アプリケーションショートカットのユースケースについて紹介します。

［スタート］メニューに何を置くか、ユーザーが選べるようにする（セルフサービス）

数十（または数百の）アプリケーションがある場合は、ユーザーがお気に入りのアプリケーションを選択して、［スタート］メニューに追加できるようにするのが最も便利です。

［スタート］メニューに置くアプリケーションをユーザーが選べるようにするには、	Receiverをセルフサービスモードに構成します。 このモードでは、「自動プロビジョニング」設定および「必須」アプリケーションキーワード設定も構成できます。
ユーザーが［スタート］メニューに置くアプリケーションを選べるようにして、また特定のアプリケーションショートカットをデスクトップに置くには、	Receiverをオプション設定なしで構成して、デスクトップに置くアプリケーションについてアプリケーションごとの設定を使用します。 必要に応じて、「自動プロビジョニング」および「必須」アプリケーションを使用します。

［スタート］メニュー内にアプリケーションショートカットなし

コンピュータを家族で共有して使用していて、アプリケーションショートカットを一切置きたくないとします。 このような場合、もっとも簡単なのはブラウザーアクセスです。いずれの構成もせずにReceiverをインストールし、Receiver for WebおよびWeb interfaceをブラウズします。 また、ショートカットをどこにも配置しないでセルフサービスアクセス用にReceiverを構成することもできます。

Receiverが［スタート］メニューに自動的にアプリケーションショートカットを配置しないようにするには、	ReceiverでPutShortcutsInStartMenu=Falseと構成します。 アプリケーションごとの設定を使ってショートカットを置かない限り、セルフサービスモードであってもReceiverにより［スタート］メニュー内にアプリケーションは配置されません。

［スタート］メニュー内、またはデスクトップ上にすべてにアプリケーションショートカットを置く

ユーザーが所有するアプリケーションが少ない場合は、そのすべてを［スタート］メニュー内やデスクトップ上に、あるいはデスクトップ上のフォルダー内に置くことができます。

Receiverによって［スタート］メニューにすべてのアプリケーションショートカットを自動的に配置する場合は、	ReceiverでSelfServiceMode =Falseと構成します。 使用可能なすべてのアプリケーションが［スタート］メニュー内に表示されます。

すべてのアプリケーションショートカットをデスクトップ上に置く場合は、	ReceiverでPutShortcutsOnDesktop = trueと構成します。 使用可能なすべてのアプリケーションがデスクトップに表示されます。
すべてのショートカットをデスクトップ上のフォルダー内に置く場合は、	ReceiverでDesktopDir=アプリケーションショートカットを置くデスクトップフォルダーの名前と構成します。

XenApp 6.5または7.xでのアプリケーションごとの設定

ショートカットの場所を指定して、すべてのユーザーが同じ場所でそれにアクセスできるようにするには、XenAppのアプリケーションごとの設定を使用します。

セルフサービスモードになっているかどうかあるいは［スタート］メニューかどうかには関係なく、アプリケーションごとの設定によりアプリケーションを配置する場所を決定する場合は、	Receiver で**PutShortcutsInStartMenu=false**と構成して、アプリケーションごとの設定を有効にします。 注：この設定は、Web Interfaceサイトにのみ適用されます。

カテゴリフォルダーまたは特定のフォルダーのアプリケーション

特定のフォルダー内にアプリケーションを表示する場合は、次のオプションを使用します。

Receiverが［スタート］メニューに置くアプリケーションショートカットを割り当てたカテゴリ（フォルダー）内に表示する場合は、	ReceiverでUseCategoryAsStartMenuPath=Trueと構成します。 注：Windows 8/8.1では、［スタート］メニュー内には階層分けされたフォルダーを作成できません。 アプリケーションは個々に、またはXexAppで定義されたカテゴリサブフォルダー内ではないルートフォルダーの下に表示されます。
Receiverが［スタート］メニューに置くアプリケーションを特定のフォルダー内に配置する場合は、	ReceiverでStartMenuDir=［スタート］メニューフォルダー名の名前と構成します。

ログオフまたは終了時にアプリケーションを削除

エンドポイントをほかのユーザーと共有していて、自分のアプリケーションがそのユーザーには表示されないようにしたい場合は、ログオフまた終了時にアプリケーションが削除されるようにすることができます。

Receiverがログオフ時にすべてのアプリケーションを削除するようにするには、	ReceiverでRemoveAppsOnLogoff=Trueと構成します。
Receiverが終了時にすべてのアプリケーションを削除するようにするには、	ReceiverでRemoveAppsOnExit=Trueと構成します。

ローカルアプリケーションアクセスのアプリケーションの構成

ローカルアプリケーションアクセスのアプリケーションを構成する場合は次のようにします。

- 説明に「KEYWORDS:prefer=""」という文字列を追加すると、Receiverでアクセスされるアプリケーションの代わりにローカルのアプリケーションが使用されるようになります。 この機能は、「ローカルアプリケーションアクセス」と呼ばれます。
  Receiverは、ユーザーのコンピューターにアプリケーションをインストールする前にで指定されたパターンを検索し、そのアプリケーションがローカルにインストールされているかどうかをチェックします。 アプリケーションがローカルにインストールされている場合、Receiverはそのアプリケーションをサブスクライブして、ショートカットは作成しません。 ユーザーがReceiverからそのアプリケーションを起動すると、ローカルにインストールされたアプリケーション（ここでは「優先アプリケーション」と呼びます）が起動します。

  ユーザーがReceiverを使用せずに優先アプリケーションをアンインストールすると、Receiverの次回更新時までそのアプリケーションのサブスクリプションは解除されます。 ユーザーがReceiverを使用して優先アプリケーションをアンインストールすると、Receiverはそのアプリケーションのサブスクリプションを解除しますが、アンインストールはしません。

  注：Receiverでアプリケーションをサブスクライブすると、キーワードpreferが適用されます。 アプリケーションをサブスクライブした後でこの文字列を追加しても、そのアプリケーションには適用されません。
  同じアプリケーションに対して複数回preferキーワードを指定できます。 この場合、指定したパターンの1つが一致すると、そのアプリケーションに設定が適用されます。 以下のパターンを任意に組み合わせて指定できます。

  - prefer="<ApplicationName>"
    ショートカットファイルに指定されているアプリケーション名にマッチします。 単語または語句を指定できますが、 語句の場合は引用句を使用する必要があります。 単語やファイルパスの一部がマッチしても無視され、大文字/小文字も区別されません。 アプリケーション名によるマッチは、管理者が手作業で設定する場合に便利です。

KEYWORDS:prefer=	**Programs配下のショートカット**	**マッチするかどうか**
Word	\Microsoft Office\Microsoft **Word** 2010	はい
"Microsoft Word"	\Microsoft Office**Microsoft Word** 2010	はい
コンソール	\McAfee\VirusScan **Console**	はい
Virus	\McAfee\VirusScan Console	いいえ
McAfee	\McAfee\VirusScan Console	いいえ

  - prefer="\\<Folder1>\<Folder2>\...\<ApplicationName>"
    ［スタート］メニューのショートカットファイルの絶対パスおよびアプリケーション名にマッチします。 Start Menuディレクトリのサブフォルダー Programs以下の絶対パスを指定します。 パスにスペースが含まれている場合は、引用符を使用する必要があります。 また、大文字と小文字は区別されます。 絶対パスによるマッチは、XenDesktopでプログラム的に優先アプリケーションを設定する場合に便利です。

KEYWORDS:prefer=	**Programs配下のショートカット**	**マッチするかどうか**
"\\Programs\Microsoft Office\Microsoft Word 2010"	**\Programs\Microsoft Office\Microsoft Word 2010**	はい
"\\Microsoft Office\"	\Programs\Microsoft Office\Microsoft Word	いいえ

KEYWORDS:prefer=	Programs配下のショートカット	マッチするかどうか
"\\Microsoft Word 2010"	\Programs\Microsoft Office\Microsoft Word 2010	いいえ
"\\Programs\Microsoft Word 2010"	**\Programs\Microsoft Word 2010**	はい

- prefer="\<Folder1>\<Folder2>\...\<ApplicationName>"
  ［スタート］メニューのショートカットファイルの相対パスにマッチします。 相対パスにはアプリケーション名を含める必要があり、そのショートカットの親フォルダー名を含めることもできます。 ショートカットのファイルパスの末尾が、指定したパターンに一致すると、そのアプリケーションに設定が適用されます。 パスにスペースが含まれている場合は、引用符を使用する必要があります。 また、大文字と小文字は区別されます。 相対パスによるマッチは、プログラム的に優先アプリケーションを設定する場合に便利です。

KEYWORDS:prefer=	Programs配下のショートカット	マッチするかどうか
"\Microsoft Office\Microsoft Word 2010"	**\Microsoft Office\Microsoft Word 2010**	はい
"\Microsoft Office\"	\Microsoft Office\Microsoft Word 2010	いいえ
"\Microsoft Word 2010"	\Microsoft Office**\Microsoft Word 2010**	はい
"\Microsoft Word"	\Microsoft Word 2010	いいえ

ほかのキーワードについては、StoreFrontのドキュメントの「ユーザーエクスペリエンスの最適化」を参照してください。

XenDesktop環境の構成

Jul 07, 2016

この記事の各トピックでは、USBサポートの構成方法、Desktop Viewerウィンドウが暗くなる機能の無効化、および複数のユーザーやデバイスのための設定について説明します。

XenDesktopおよびXenApp接続のUSBサポートの構成

USBサポート機能により、ユーザーが仮想デスクトップ上で作業しているときにさまざまな種類のUSBデバイスを使用できるようになります。 ユーザーがコンピューターにUSBデバイスを接続すると、仮想デスクトップ内でそのデバイスを操作できるようになります。 この機能では、フラッシュドライブ、スマートフォン、PDA、プリンター、スキャナー、MP3プレーヤー、セキュリティデバイス、およびタブレットなどのUSBデバイスがサポートされます。 Desktop Viewerのユーザーは、ツールバーの基本設定を使用して、仮想デスクトップでUSBデバイスを使用できるようにするかどうかを制御できます。

Webカメラ、マイク、スピーカー、およびヘッドセットなどのUSBデバイスのアイソクロナス機能は、一般的な高速LAN環境でサポートされます。 これにより、Microsoft Office CommunicatorやSkypeなどのパッケージでこれらのデバイスを使用できるようになります。

以下の種類のデバイスは直接サポートされるため、XenDesktopおよびXenAppセッションでUSBサポート機能は使用されません。

- キーボード
- マウス
- スマートカード

注：特殊用途のUSBデバイス（Bloombergキーボードや3-Dマウスなど）では、USBサポート機能が使用されるように構成できます。 Bloombergキーボードの構成について詳しくは、「Bloombergキーボードの構成」を参照してください。 そのほかの特殊用途のUSBデバイスのポリシー規則の構成について詳しくは、CTX120292を参照してください。
デフォルトでは、特定の種類のUSBデバイスがXenDesktopおよびAppsセッションで動作しないように設定されています。 たとえば、内部USBでシステムボードに装着されたネットワークインターフェイスカードは、 このデバイスのリモート操作は通しません。 次の種類のUSBデバイスは、XenDesktopセッションでの使用をデフォルトでサポートしていません。

- Bluetoothドングル
- 統合ネットワークインターフェイスカード
- USBハブ
- USBグラフィックアダプター

USBハブに接続されたデバイスは仮想デスクトップで使用できますが、USBハブ自体はリモート処理できません。

次の種類のUSBデバイスは、XenAppセッションでの使用をデフォルトでサポートしていません。

- Bluetoothドングル
- 統合ネットワークインターフェイスカード
- USBハブ
- USBグラフィックアダプター
- オーディオデバイス
- マスストレージデバイス

ユーザーが使用できるUSBデバイスの範囲を変更する方法については、 「仮想デスクトップで使用できるUSBデバイスの一覧の変更」を参照してください。

特定のUSBデバイスを自動的にリダイレクトする方法については、CTX123015を参照してください。

USBサポートのしくみ

ユーザーがエンドポイントにUSBデバイスを接続すると、USBポリシーが照合され、許可されているデバイスであることが認識されると、仮想デスクトップ上で使用可能になります。 USBポリシーで拒否されるデバイスは、ローカルのデスクトップ」でのみ使用可能になります。

USBデバイスを接続すると、新しいデバイスについて知らせる通知が表示されます。 ユーザーは、USBデバイスを接続するたびに、そのデバイスを仮想デスクトップで使用するかどうかを選択できます。 ユーザーは、仮想デスクトップセッションの開始前、またはセッション実行中に接続したUSBデバイスが、フォーカスのある仮想デスクトップで自動的に使用可能になるように設定することもできます。

マスストレージデバイス

マスストレージデバイス（大容量記憶装置）の場合は、USBサポートに加え、クライアント側ドライブのマッピング機能によるリモートアクセスも可能で、これは［Citrix Receiver］>［Remoting client devices］>［Client drive mapping］で設定します。 このポリシーを適用すると、ユーザーのログオン時にユーザーデバイス上のドライブが自動的に仮想デスクトップ上のドライブ文字にマップされます。 これらのドライブは、マップされたドライブ文字を持つ共有フォルダーとして表示されます。

クライアント側リムーバブルドライブマッピングとUSBサポートの2つの設定の主な違いは以下のとおりです。

機能	クライアント側ドライブのマッピング	USBサポート
デフォルトで有効。	はい	いいえ
読み取り専用アクセスの構成が可能	はい	いいえ
セッション中にデバイスを安全に取り外せる	いいえ	はい（ユーザーが通知領域の［ハードウェアの安全な取り外し］をクリックする場合）

［Generic USB］と［Client drive mapping］の両方のポリシーが有効で、マスストレージデバイスがセッションの開始前に装着された場合は、USBサポート機能によるリダイレクトの前にクライアント側ドライブのマッピングによるリダイレクトが実行されます。 マスストレージデバイスがセッションの開始後に装着された場合は、クライアント側ドライブのマッピングのにUSBサポートによるリダイレクトが実行されます。

デフォルトで許可されるUSBデバイスのクラス

以下のクラスのUSBデバイスは、デフォルトのUSBポリシー規則により仮想デスクトップでの使用が許可されます。

この一覧に記載されていても、一部のクラスは構成を追加しなければXenDesktopおよびXenAppセッションでリモート処理ができません。 それらのクラスについては以下に記述します。

- オーディオ（クラス01）。 このクラスのデバイスとして、オーディオ入力デバイス（マイク）、オーディオ出力デバイス、およびMIDIコントローラーがあります。 最近のオーディオデバイスでは一般的にアイソクロナス転送が使用されますが、この機能はXenDesktop 4以降でサポートされます。 USBサポートを使用するXenAppでオーディオデバイスをリモート操作できないため、オーディオ（クラス01）はXenAppに適用できません。
  注：VoIP電話などの一部の特殊デバイスには追加の構成が必要です。 手順については、CTX123015を参照してください。

- 物理インターフェイスデバイス（クラス05）。 このデバイスはヒューマンインターフェイスデバイス（HID）と似ていますが、一般的に「リアルタイム」の入力またはフィードバックを提供し、フォースフィードバックジョイスティック、モーションプラットフォーム、およびフォースフィードバックエクソスケルトンなどがあります。
- 静止画（クラス06）。 このクラスのデバイスとして、デジタルカメラおよびスキャナーがあります。 ほとんどのデジタルカメラは、画像転送プロトコル（PTP）またはメディア転送プロトコル（MTP）を使ってコンピューターやほかの周辺機器にイメージを転送する静止画クラスをサポートします。 また、デジタルカメラはマスストレージデバイスとして機能する場合もあり、カメラ自体のメニューを使っていずれかのクラスを使用するように構成できます。
  カメラがマスストレージデバイスとして機能する場合はクライアントドライブマッピングが使用され、USBサポートは必要ありません。

- プリンター（クラス07）。 一部のプリンターではベンダー固有のプロトコル（クラスff）が使用されますが、一般的にはこのクラスにほとんどのプリンターが含まれます。 マルチ機能プリンターの場合は、USBハブが内蔵されていたり、混合デバイスであったりする場合があります。 いずれの場合も、印刷機能では一般的にプリンタークラスが使用され、スキャナーやFAX機能では静止画などの別のクラスが使用されます。
  プリンターは通常、USBサポートなしで適切に動作します。

  注：このクラスのデバイス（特にスキャナー機能を持つプリンター）には追加の構成が必要です。 手順については、CTX123015を参照してください。
- マスストレージ（クラス08）。 最も一般的なマスストレージデバイス（大容量記憶装置）として、USBフラッシュドライブがあります。そのほかには、USB接続のハードドライブ、CD/DVDドライブ、およびSD/MMCカードリーダーがあります。 また、内部ストレージを持つさまざまなデバイスがあり、これらもこのクラスのインターフェイスを提供します。たとえば、メディアプレーヤー、デジタルカメラ、携帯電話などがあります。 USBサポートを使用するXenAppでマスストレージデバイスをリモート操作できないため、マスストレージ（クラス08）はXenAppに適用できません。 既知のサブクラスには次のものが含まれます。
  - 01 制限付きフラッシュデバイス
  - 02 一般的なCD/DVDデバイス（ATAPI/MMC-2）
  - 03 一般的なテープデバイス（QIC-157）
  - 04 一般的なフロッピーディスクドライブ（UFI）
  - 05 一般的なフロッピーディスクドライブ（SFF-8070i）
  - 06 ほとんどのマスストレージデバイスはこのSCSIのバリエーションを使用します

  マスストレージデバイスには、クライアントドライブマッピングを介して頻繁にアクセスすることができ、USBサポートは必要ありません。

  重要：ウィルスプログラムの中には、あらゆる種類のマスストレージデバイスを媒体にして活発に増殖するものがあります。 クライアントドライブマッピングまたはUSBサポート機能でマスストレージデバイスの使用を許可する場合は、ビジネス上の必要性があるかどうかを慎重に考慮してください。
- コンテンツセキュリティ（クラス0d）。 通常、ライセンスまたはデジタル権利の管理のためのコンテンツ保護を実行します。 このクラスのデバイスとして、ドングルがあります。
- ビデオ（クラス0e）。 このクラスのデバイスとして、ビデオ、Webカメラ、デジタルカムコーダー、アナログビデオ変換機、一部のテレビチューナー、およびビデオストリーミングをサポートする一部のデジタルカメラなど、ビデオ関連の機器があります。
  注：ほとんどのビデオストリーミングデバイスではアイソクロナス転送が使用されますが、この機能はXenDesktop 4以降でサポートされます。 動作検知機能付きのWebカメラなど、一部のビデオデバイスには追加の構成が必要です。 手順については、CTX123015を参照してください。
- パーソナルヘルスケア（クラス0f）。 このデバイスには、血圧センサー、心拍数モニター、万歩計、薬剤モニター、肺活量計などの個人用健康器具があります。
- アプリケーションおよびベンダー固有（クラスfeおよびff）。 多くのデバイスがベンダー独自のプロトコルまたはUSBコンソーシアムで標準化されていないプロトコルを使用しており、これらは通常はベンダー固有（クラスff）として分類され

す。

デフォルトで拒否されるUSBデバイスのクラス

次のUSBデバイスの異なるクラスは、デフォルトのUSBポリシー規則により拒否されます。

- 通信およびCDCコントロール（クラス02および0a）。仮想デスクトップ自体への接続にこれらのデバイスのいずれかが使用される場合があるため、デフォルトのUSBポリシーではこれらのデバイスのリモートでの実行は許可されていません。
- ヒューマンインターフェイスデバイス（クラス03）。さまざまな種類の入出力デバイスを含みます。 一般的なヒューマンインターフェイスデバイス（HID）として、キーボード、マウス、ポインティングデバイス、グラフィックタブレット、センサー、およびゲームのコントローラー、ボタン、およびコントロール機能などがあります。
  サブクラス01は「起動インターフェイス」クラスとして知られ、キーボードおよびマウスで使用されます。

  デフォルトのUSBポリシーはUSBキーボード（クラス03、サブクラス01、プロトコル1）またはUSBマウス（クラス03、サブクラス01、プロトコル2）を許可しません。 これは、ほとんどのキーボードおよびマウスはUSBサポートなしでも適切に処理され、一般に仮想デスクトップ内だけでなくローカルでも使用されるためです。

- USBハブ（クラス09）。USBハブを使用すると、より多くのデバイスをローカルのコンピューターに接続できます。 これらのデバイスにリモートでアクセスする必要はありません。
- スマートカード（クラス0b）。 スマートカードリーダーには、非接触型および接触型のスマートカードリーダーと、スマートカードと同等のチップを埋め込んだUSBトークンがあります。
  スマートカードリーダーは、スマートカードサポート機能によりアクセスできるため、USBサポートは必要ありません。

- ワイヤレスコントローラー（クラスe0）。これらのデバイスの中には、重要なネットワークアクセスを提供していたり、Bluetoothキーボードやマウスなどの基幹周辺装置を接続していたりするものがある場合があります。
  デフォルトのUSBポリシーはこれらのデバイスを許可していません。 ただし、USBサポートを使ったアクセスに適したデバイスもあります。

- **そのほかのネットワークデバイス（クラスef、サブクラス04）**。 これらのデバイスの一部に、重要なネットワークアクセスを提供している可能性があるものがあります。 デフォルトのUSBポリシーはこれらのデバイスを許可していません。 ただし、USBサポートを使ったアクセスに適したデバイスもあります。

仮想デスクトップで使用できるUSBデバイスの一覧の変更

icaclient_usb.admファイルを編集して、仮想デスクトップセッション内で使用できるUSBデバイスの範囲を更新できます。 これにより、グループポリシーを使用してReceiverに変更を加えることができます。 このファイルは、次のインストールフォルダーにあります。

<ルートドライブ>:\Program Files\Citrix\ICA Client\Configuration\en

または、各ユーザーデバイスのレジストリに次のレジストリキーを追加できます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB 種類=文字列 名前="DeviceRules" 値=

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。
製品のデフォルトの規則は、次の場所に保存されています。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB 種類=複数行文字列値 名前="DeviceRules" 値=

これらのデフォルトの規則は変更しないでください。

これらの規則およびその構文については、http://support.citrix.com/article/ctx119722/を参照してください。

Bloombergキーボードの構成

Bloombergキーボードは、XenDesktopおよびXenAppセッションでサポートされます（ただしほかのUSBキーボードはサポートされません）。 プラグインをインストールすると必要なコンポーネントが自動的にインストールされますが、インストール時または後でレジストリキーを変更しなければ、この機能は有効になりません。

単一のユーザーデバイス上の複数のセッションでBloombergキーボードを使用しないでください。 このキーボードは単一セッション環境でのみ正しく動作します。

Bloombergキーボードのサポートを有効または無効にするには

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. レジストリで次のキーを検索します。
   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

2. 次のいずれかを行います。
   - この機能を有効にするには、種類がDWORDで名前がEnableBloombergHIDの値のデータを1に設定します。
   - この機能を無効にするには、値のデータを0に設定します。

非アクティブなDesktop Viewerウィンドウの減光を無効にするには

Desktop Viewerの複数のウィンドウを使用する場合、デフォルトではアクティブでないウィンドウが減光されます。 この機能により、複数のデスクトップを同時に表示する必要がある場合は、非アクティブなデスクトップ上の情報が読みづらくなる可能性があります。 レジストリを編集してデフォルトの設定を無効にし、Desktop Viewerウィンドウの減光を防ぐことができます。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. ユーザーデバイスで、DisableDimmingという名前のREG_DWORDエントリを次のキーのどちらかに作成します。作成場所は減光を無効にする対象が現在のデバイスユーザーかデバイス自体かによって異なります。 デバイスでDesktop Viewerを使用したことがある場合は、エントリが既に存在します。

   - HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer
   - HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer

   または、ユーザーまたはデバイスの設定で減光を制御する代わりに、同じREG_WORDエントリを次のキーのどちらかに作成することによって、ローカルポリシーを定義できます。

   - HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer
   - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer

   通常、プラグイン管理者やユーザーではなくXenDesktop管理者がグループポリシーを使用してポリシー設定を制御するので、これらのキーを使用するかどうかは任意です。 そのため、これらのキーを使用する前に、XenDesktop管理者がこの機能のポリシーを設定しているかどうか確認してください。

2. エントリを1またはtrueのような0以外の値に設定します。

エントリが未指定、または0に設定されている場合は、Desktop Viewerウィンドウが減光します。 複数のエントリが指定されている場合、次の方法が使用されます。 次の一覧の上位のエントリの値によって、ウィンドウを減光するかどうかが決まります。

1. HKEY_CURRENT_USER\Software\Policies\Citrix\...
2. HKEY_LOCAL_MACHINE\Software\Policies\Citrix\...
3. HKEY_CURRENT_USER\Software\Citrix\...
4. HKEY_LOCAL_MACHINE\Software\Citrix\...

複数のユーザーおよびデバイスの設定を構成するには

Receiverのユーザーインターフェイスに表示されるオプションでの構成に加えて、グループポリシーエディターやicaclient.admテンプレートファイルを使って設定を構成できます。 グループポリシーエディターでは、以下の構成を行えます。

- icaclient.admファイルを編集して、すべてのReceiver設定をicaclientテンプレートで構成する。 ADMファイルの編集および特定のコンピューターに設定を適用する方法について詳しくは、Microsoft社のグループポリシーに関するドキュメントを参照してください。
- クライアントデバイスの特定のユーザーまたはすべてのユーザーに構成を適用する。
- 複数のユーザーデバイスに構成を適用する。

グループポリシーを使用してリモートからユーザーデバイスを設定することをお勧めします。ただし、必要なレジストリエントリをアップデートできるのであれば、レジストリエディターなどを使用して構成することもできます。

1. 管理者として、［スタート］メニューからgpedit.mscを実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。

   注：既にicaclientテンプレートをグループポリシーオブジェクトエディターにインポートしている場合、手順2.～5.は省略できます。
2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、ReceiverのConfigurationフォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、icaclient.admを選択します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. ［ユーザーの構成］または［コンピューターの構成］で、必要に応じて設定の変更を行います。

StoreFrontの構成

Jul 22, 2016

Citrix StoreFrontは、XenDesktop、XenApp、およびVDI-in-a-Boxのユーザーを認証し、使用可能なデスクトップおよびアプリケーションをストアに集約して、Receiverユーザーに提供します。

ここで説明する構成手順に加えて、リモートユーザー（インターネットを介して接続するユーザーや遠隔地のユーザーなど）が内部ネットワークにアクセスできるようにNetScaler GatewayまたはAccess Gatewayを構成する必要もあります。

> **注意**
>
> Citrix Receiver for Windowsで、すべてのアカウントを表示するオプションを選択すると、更新されたStoreFrontユーザーインターフェイスではなく、以前のStoreFrontユーザーインターフェイス（緑のバブルテーマ）が常に表示されます。

StoreFrontを構成するには

1. StoreFrontのドキュメントを参照して、StoreFrontをインストールして構成します。Receiver for Windowsを使用するには、HTTPS接続が必要です。 StoreFrontサーバーでHTTPが構成されている場合は、ユーザーデバイス上のレジストリキーを設定する必要があります。詳しくは、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」のALLOWADDSTOREプロパティに関する説明を参照してください。
   注：独自のReceiverダウンロードサイトを作成する管理者用に、テンプレートが提供されています。

ワークスペースコントロール再接続の管理

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのアプリケーションでの作業を継続できます。 これにより、たとえば病院で臨床医がほかのワークステーションに移動しても、移動先のデバイスでアプリケーションを起動し直す必要がなくなります。 Receiver for Windowsの場合、レジストリを変更してクライアントデバイスのワークスペースコントロールを管理します。 これはまた、グループポリシーを使用するドメイン参加クライアントデバイスに対しても実行できます。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

WSCReconnectModeUserを作成し、既存のレジストリキーWSCReconnectModeをMaster Desktop ImageまたはXenAppサーバーホストで変更します。 公開デスクトップはReceiverの動作を変更できます。

Windows ReceiverのWSCReconnectModeキー設定：

- 0 = いずれに既存のセッションにも再接続しない
- 1 = アプリケーションの起動時に再接続する
- 2 = アプリケーションの更新時に再接続する
- 3 = アプリケーションの起動または更新時に再接続する
- 4 = Receiverインターフェイスを開いたときに再接続する
- 8 = Windowsログオン時に再接続する
- 11 = 3と8の組み合わせ

Windows Receiverに対するワークスペースコントロールの無効化

Windows Receiverに対してワークスペースコントロールを無効にするには、次のキーを作成します：

HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle（64ビット）

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle （32ビット）

値の名前：**WSCReconnectModeUser**

種類：REG_SZ

値のデータ：0

次のキーをデフォルト値の3から0に変更

HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle（64ビット）

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle （32ビット）

値の名前：**WSCReconnectMode**

種類：REG_SZ

値のデータ：0

注：新しいキーを作成しない代わりに、REG_SZ値のWSCReconnectAllをfalseに設定することができます。

状態インジケータータイムアウトの変更

ユーザーがセッションを起動しているときに状態インジケーターが表示される時間を変更できます。 タイムアウト期間を変更するには、REG_DWORD値のSI INACTIVE MSをHKLM\SOFTWARE\Citrix\ICA CLIENT\Engine\で作成します。 状態インジケーターをすぐに非表示したい場合は、REG_DWORD値を4に設定します。

> ### 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

グループポリシーオブジェクトテンプレートによるReceiverの構成

Jan 27, 2017

GPOを介したストアの追加または指定

グループポリシーオブジェクトを使用する方法が推奨されており、Citrix Receiver for Windows関連の設定を構成するテンプレートファイル（OSに応じてreceiver.admまたはreceiver.admx\receiver.adml）が提供されています。

> ### 注意
> receiver.admx/receiver.admlは、Windows VistaとWindows Server 2008以降で使用できます。 ADMファイルは、Windows XP Embeddedプラットフォームでのみ使用できます。

> ### 注意
> VDAのインストールを通じてCitrix Receiver for Windowsを構成した場合、admx/admlファイルはインストールディレクトリにあります。 たとえば、<インストールディレクトリ>\online plugin\Configurationです。

Citrix Receiver for Windowsの各テンプレートファイルとその配置場所については以下の表を参照してください。

ファイルの種類	ファイルの場所
receiver.adm	<インストールディレクトリ>\ICA Client\Configuration
receiver.admx	<インストールディレクトリ>\ICA Client\Configuration
receiver.adml	<インストールディレクトリ>\ICA Client\Configuration\[MUIカルチャ]

> ### 注意
> 最新のCitrix Receiver for Windowsに付属のテンプレートファイルを使用することをお勧めします。 最新のファイルをインポートしても、以前の設定は保持されます。

ローカルGPOにadmテンプレートファイルを追加するには

注：admテンプレートファイルを使用して、ローカルGPOやドメインベースのGPOを構成できます。

1. 管理者として、［スタート］メニューからgpedit.mscを実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。
注：既にCitrix Receiver for Windowsのテンプレートをグループポリシーオブジェクトエディターにインポートしている場合、手順2.～5.は省略できます。
2. グループポリシーエディターの左ペインで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］をクリックし、テンプレートファイルの場所（<インストールディレクトリ>\ICA Client\Configuration\receiver.adm）を参照します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
ローカルGPOのパス［管理用テンプレート］>［従来の管理用テンプレート（ADM）］>［Citrixコンポーネント］>［Citrix Receiver］に、Citrix Receiver for Windowsのテンプレートファイルが追加されます。
ローカルGPOにadmテンプレートファイルが追加されると、次のメッセイジが表示されます。
「[strings]セクションの次のエントリが長すぎるため切り詰められました。
［OK］をクリックしてメッセージを無視します。

ローカルGPOにadmx/admlテンプレートファイルを追加するには

注：admx/admlテンプレートファイルを使用して、ローカルGPOやドメインベースのGPOを構成できます。 ADMXファイルの管理については、こちらのMicrosoft MSDNの記事を参照してください。
1. Citrix Receiver for Windowsをインストールしてから、テンプレートファイルをコピーします。

admx：
コピー元：<インストールディレクトリ>\ICA Client\Configuration\receiver.admx
コピー先：%systemroot%\policyDefinitions

adml：
コピー元：<インストールディレクトリ>\ICA Client\Configuration\[MUIculture]receiver.adml
コピー先：%systemroot%\policyDefinitions\[MUIculture]

［管理用テンプレート］>［Citrixコンポーネント］>［Citrix Receiver］のローカルGPOに、Citrix Receiver for Windowsのテンプレートファイルが追加されます。

グループポリシーオブジェクトの icaclient.admテンプレートを使って、ネットワークのルーティング、プロキシサーバー、信頼されるサーバーの設定、ユーザーのルーティング、リモートユーザーデバイス、およびユーザーエクスペリエンスに関する規則を構成することをお勧めします。

icaclient.admテンプレートファイルをドメインポリシーおよびローカルコンピューターのポリシーと一緒に使用できます。 ドメインポリシーの場合、グループポリシー管理コンソールを使ってテンプレートファイルをインポートします。 これは組織全体に存在する多くの異なるユーザーデバイスにCitrix Receiverの設定を適用するのに非常に有用です。 単一のユーザーデバイスの場合は、デバイス上のローカルのグループポリシーエディターを使ってテンプレートをインポートします。

グループポリシーオブジェクトテンプレートによるReceiverの構成

> **注意**
>
> 最新のCitrix Receiverと共に提供されるGPOテンプレートファイルを使用することをお勧めします。 最新のファイルをインポートして

も、以前の設定は保持されます。

TLSおよびグループポリシーについて

このポリシーを使用してTLSオプションを構成します。このオプションにより、Citrix Receiverで接続先のサーバーを安全に識別して、サーバーとのすべての通信を暗号化できます。 信頼されていないネットワークを介する接続ではTLSを使用することをお勧めします。 ReceiverとXenAppまたはXenDesktopの間では、TLS 1.0、TLS 1.1、およびTLS 1.2プロトコルがサポートされます。

このポリシーが有効な場合、［Require SSL for all connections］チェックボックスをオンにすることによって、公開アプリケーションおよびデスクトップに対するReceiverのすべての通信で強制的にTLSを使用させることができます。

Citrix Receiverでは、サーバーにより提示されるセキュリティ証明書上の名前でサーバーを識別します。 これはDNS名の形式です（例：www.citrix.com）。 Receiverが特定のサーバーにのみ接続するように制限することができます。これは、［Allowed SSL servers］設定のコンマ区切りの一覧にサーバーを指定することによって行います。 ここでワイルドカードとポート番号を指定できます。たとえば、「*.citrix.com:4433」により、共通名が「.citrix.com」で終わるどのサーバーともポート4433での接続が許可されます。 セキュリティ証明書の情報の正確さは証明書の発行元により言明されます。 Receiverで証明書の発行元が認識されず信頼されない場合は、接続が拒否されます。

TLSで接続する場合、ReceiverにReceiver自体を識別するセキュリティ証明書の提供を要求するようにサーバーを構成できます。 ［Client Authentication］設定を使用して、識別を自動的に行うかユーザーに通知するかを構成します。 次のオプションがあります。

- never supply identification
- only use the certificate configured here
- to always prompt the user to select a certificate
- to prompt the user only if there a choice of certificate to supply

ヒント

［Client Certificate］設定を使用して、識別証明書の拇印を指定します。これにより、ユーザーに不要なプロンプトを表示しないようにすることができます。

サーバーのセキュリティ証明書の検証時に証明書の発行元と通信して証明書失効一覧（CRL）を取得するように、プラグインを構成することができます。これにより、サーバー証明書が失効していないことを保証します。 これにより、システムが危険にさらされている場合は発行元が証明書を無効にすることができます。 ［CRL verification］設定を使用してプラグインを以下のいずれかに構成します。

- not check CRLs at all
- only check CRLs that have been previously obtained from the issuer
- actively retrieve an up-to-date CRL
- to refuse to connect unless it can obtain an up-to-date CRL

さまざまな製品に対してTLSを構成する組織では、Citrixプラグイン向けのサーバーを識別することを選択できます。これは、セキュリティ証明書の一部として証明書ポリシーのOIDを指定して行います。 ポリシーのOIDをここで構成する場合は、互換性のあるポリシーを宣言する証明書のみがReceiverで受け入れられるようになります。

一部のセキュリティポリシーには、接続に使用される暗号アルゴリズムに関連する要件があります。 [TLS version] 設定を使用して、TLS v1.0、TLS 1.1、およびTLS 1.2のみを使用するようにプラグインに制限をかけることができます。 同様に、特定の暗号の組み合わせのみを使用するようにプラグインに制限をかけることができます。 指定できる暗号の組み合わせは以下のとおりです。

行政機関向けの暗号の組み合わせ

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384

営利企業向けの暗号の組み合わせ

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_AES_128_GCM_SHA256

FIPSセキュリティ標準の準拠

Citrix Receiver for Windows 4.4では、TLSとFIPS（Federal Information Processing Standards）を構成するための準拠モード構成オプションが導入されています。 この機能を使って、すべてのICAコネクションに対してFIPS（Publication 140-2）準拠の暗号化のみが使用されるようにします。

新しいセキュリティ準拠モードではNIST SP 800-52がサポートされます。 デフォルトでは、このモードは無効になっています（［なし］に設定）。

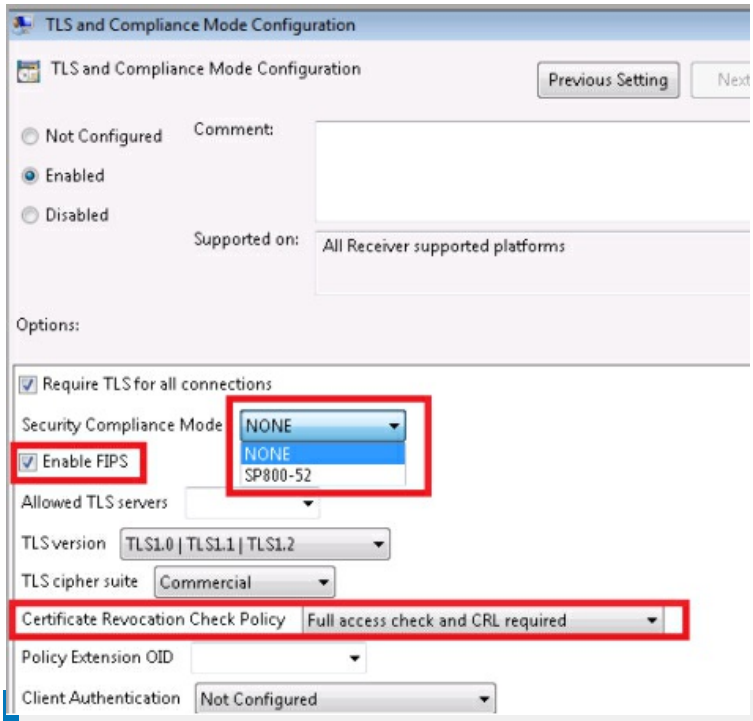
> **注意**
>
> NIST SP 800-52の準拠に必要な情報については、NIST page describing guidelines for TLS implementationsを参照してください。

またこのバージョンのCitirx Receiverにより、ICAコネクション用のTLSプロトコルを決定するTLSバージョンを定義できます。クライアントとサーバー間で相互に使用できる最新のバージョンが選択されます。

これらの機能を使用する場合、TLSおよび準拠モード構成画面で次のことを実行します。

- FIPSを有効にするチェックボックスを使用して、すべてのICAセッションに対して承認した暗号化を使用します。
- セキュリティコンプライアンスモードをSP 800-52に設定します。
- TLSのバージョンを選択します。

次の図はFIPSオプションを示しています。



> **注意**
>
> デフォルトでは、FIPSは無効（チェックなし）になっています。

FIPSの構成

すべてのICAクライアント間のFIPS暗号化を構成するには

1. ［コンピュータの構成］>［管理用テンプレート］>［Citrix Components］>［Network Routing］>**［TLS and Compliance Mode Configuration］**の順に選択します。
2. ［TLS and Compliance Mode Configuration］画面で**［Enable FIPS］**を選択します。
3. ［Security Compliance Mode］セクションで、ドロップダウンメニューから**［SP 800-52］**を選択します。 このオプションを構成する場合は、次のようにします。
   - SP 800-52準拠モードはFIPSコンプライアンスを必要とします。SP 800-52が有効になると、FIPS設定とは関係なくFIPSモードも有効になります。
   - Certificate Revocation Checkポリシーは［Full access check and CRL required］または［Full access check and CRL required all］に設定します。
4. ICAコネクションに適したTLSプロトコルのバージョンを選択します。クライアントとサーバー間で相互に使用できる最新のバージョンを選択します。次のオプションがあります。
   - TLS 1.0 | TLS 1.1 | TLS 1.2（デフォルト）
   - TLS 1.1 | TLS 1.2
   - TLS 1.2

ADMXテンプレートの使用について

StoreFront 3.0およびCitrix Receiver 4.3のリリースと共に、Citrix XenAppおよびXenDesktopで、Microsoftの新しいファイル形式であるADMXファイルがサポートされるようになりました。ADMXはレジストリベースのポリシー設定を表示するための形式で、標準に基づくXMLファイル形式を使用します。

Windows Vista/Windows Server 2008以降は、独自のマークアップ言語が使用されていたADMファイルが、これらの新しいファイルで置き換えられます。 ADMファイルはWindows XP Embeddedプラットフォームで依然として使用できます。 使用する管理ツール、グループポリシーオブジェクトエディターおよびグループポリシー管理コンソールに変更はほとんどありません。 多くの場合、日常的なグループポリシー管理タスクの実行中にADMXファイルの存在に気付くことはありません。

新しいADMXファイルを使用する主な利点の1つは、セントラルストアです。 セントラルストアはデフォルトでは使用されませんが、このオプションはドメインベースのGPOの管理で使用できます。 以前のADMファイルとは異なり、グループポリシーオブジェクトエディターでADMXファイルが各編集済みGPOにコピーされることはありませんが、ドメインコントローラー上の単一のドメインレベルの場所であるsysvol（ユーザーは構成できません）、またはセントラルストアが使用できない場合はローカルの管理用ワークステーションから読み取ることができます。 カスタムADMXファイルをセントラルストアにコピーすると共有できます。セントラルストアによって、ドメイン内のすべてのグループポリシー管理者に対してファイルが自動的に利用可能になります。 この機能により、ポリシー管理が簡素化され、GPOファイルの格納が最適化されます。

ADMXファイルは、言語に依存しない（ADMX）リソースと言語固有の（ADML）リソースに分かれており、すべてのグループポリシー管理者が利用できます。 これらの要素により、グループポリシーツールでユーザーインターフェイスが管理者の構成済み言語に応じて調整されます。

> ### 注意
>
> 詳しくは、ADMXファイルの管理についてのMicrosoft MSDNの記事を参照してください。

ADMXおよびADMLファイルの名前と場所

（以前のバージョンのReceiverで提供されていた）ADMファイルの命名規則が向上しました。 以下の表に、ADMファイルと新しいADMXファイルの名前のマッピングを示します：

Citrix Receiverのバージョン（4.3未満）	Citrix Receiverのバージョン（4.3以降）
Icaclient.adm	receiver.admx \ receiver.adm
Icaclient_usb.adm	receiver_usb.admx \ receiver_usb.adm
ica-file-signing.adm	ica-file-signing.admx \ ica-file-signing.admx
HdxFlash-Client.adm	HdxFlash-Client.admx \ HdxFlash-Client.admx

> ### 注意
>
> Windows Vista/Windows Server 2008以降では.admxファイルを、そのほかのプラットフォームでは.admファイルを使用します。

Citrix Receiverのインストーラーにより配布されるカスタムADMXおよびADMLファイルをセントラルストアにコピーして、ドメイン内のすべてのグループポリシー管理者に対してファイルを自動的に利用可能にすることができます。 以下の表に、

ADMXおよびADMLファイルをコピーする必要がある場所を示します。

ファイルの種類	ファイルの場所
receiver.admx	<インストールディレクトリ>\ICA Client\Configuration
ica-file-signing.admx	<インストールディレクトリ>\ICA Client\Configuration
receiver_usb.admx	<インストールディレクトリ>\ICA Client\Configuration\en
HdxFlash-Client.admx	<インストールディレクトリ>\ICA Client\Configuration
receiver.adml	<インストールディレクトリ>\ICA Client\Configuration
ica-file-signing.adml	<インストールディレクトリ>\ICA Client\Configuration
receiver_usb.adml	<インストールディレクトリ>\ICA Client\Configuration\en
HdxFlash-Client.adml	<インストールディレクトリ>\ICA Client\Configuration\[MUIカルチャ]

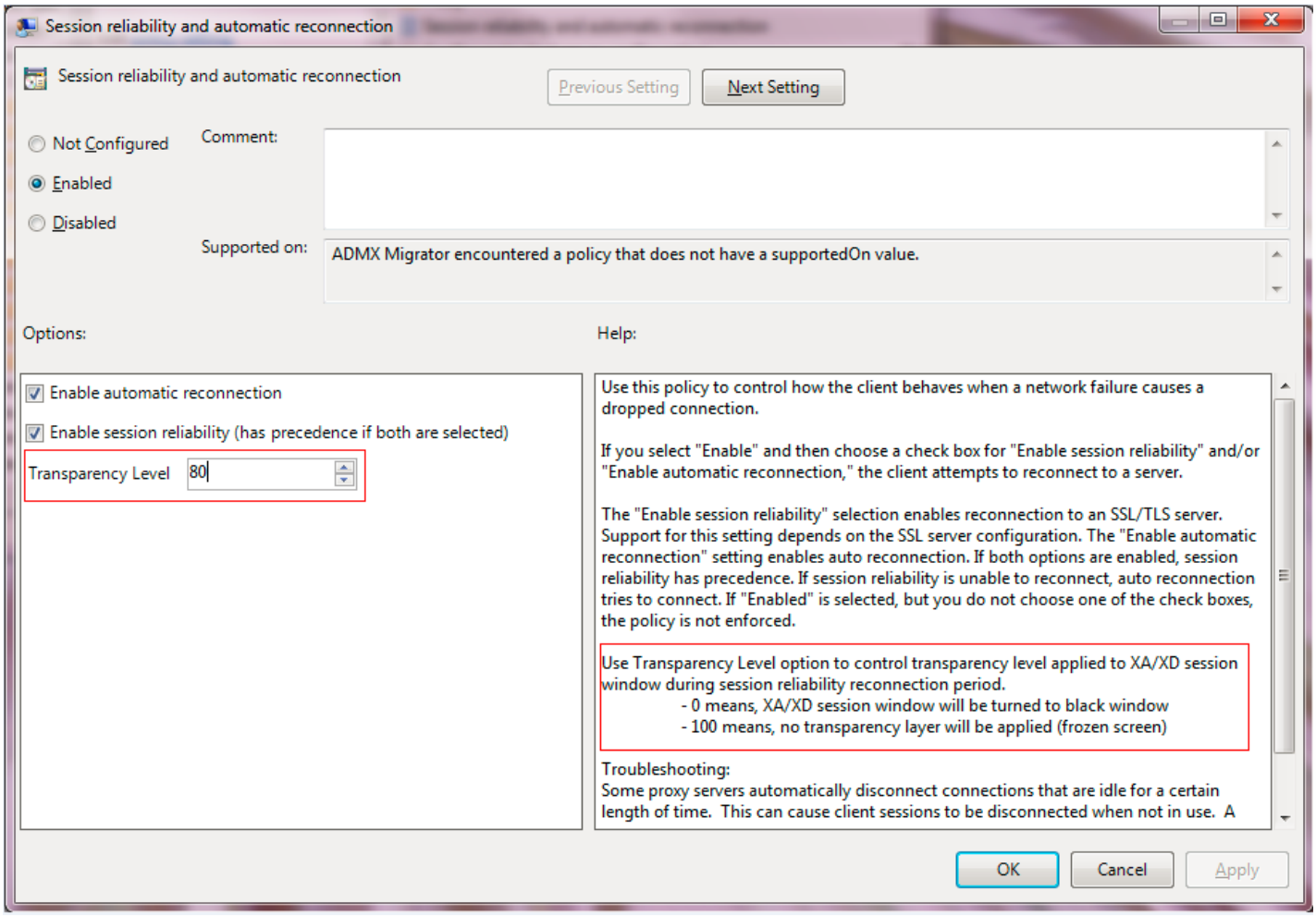
> **注意**
>
> VDAのインストールを通じてCitrix Receiverを構成する場合、ADMX/ADMLファイルはインストールディレクトリに見つかります。 たとえば、<インストールディレクトリ>\online plugin\Configurationです。

セッション画面の保持グループポリシー

セッション画面の保持グループポリシーを構成する場合、透過性レベルを設定します。 このオプションを使用すると、セッション画面の保持再接続期間の間に公開アプリケーション（またはデスクトップ）に適用される透過性レベルを制御できます。

透過性レベルを構成するには、**［コンピューターの構成］＞［管理者テンプレート］＞［Citrix Components］＞［Network Routing］＞［Session reliability and automatic reconnection］＞［Transparency Level］**の順に選択します。

> **注意**
>
> デフォルトでは、［Transparency Level］が［80］と設定されています。



ユーザーへのアカウント情報の提供

Feb 02, 2016

管理者は、ユーザーにアカウントの情報を提供します。ユーザーは、この情報を使用して仮想デスクトップやアプリケーションにアクセスします。 次の方法でユーザーに情報を提供できます。

- メールアドレスによるアカウント検出を構成する
- ユーザーにプロビジョニングファイルを提供する
- アカウント情報をユーザーに手入力させる

> **Important**
>
> Citrix Receiverを初めて使用するユーザーには、Receiverのインストール後にReceiverを再起動するよう指示してください。 これにより、ユーザーがアカウントを追加できるようになり、インストール時に一時停止状態だったUSBデバイスが認識されます。

メールアドレスによるアカウント検出を構成する

管理者がメールアドレスによるアカウント検出機能を有効にした場合、ユーザーはReceiverの初期設定時にサーバーのURLの代わりに自分のメールアドレスを入力できます。 DNS（Domain Name System）サービス（SRV）レコードにより、そのメールアドレスに関連付けられているNetScaler Gateway、Access Gateway、またはStoreFrontサーバーが自動的に検出され、仮想デスクトップやアプリケーションにアクセスするためのログオンを求めるメッセージが表示されます。

> **注意**
>
> メールアドレスによるアカウント検出は、Web Interface環境では使用できません。

メールアドレスによるReceiverアカウントの検出機能が正しく動作するようにDNSサーバーを構成する方法については、StoreFrontのドキュメントの「メールによるアカウント検出を構成する」を参照してください。

NetScaler Gatewayを構成する方法については、NetScaler Gatewayのドキュメントの「Connecting to StoreFront by using email-based discovery」を参照してください。

ユーザーにプロビジョニングファイルを提供する

StoreFrontにより提供されるプロビジョニングファイルを使用して、ユーザーはストアに接続できます。

- 管理者は、StoreFrontを使用して、接続の詳細情報を定義したプロビジョニングファイルを作成できます。 作成したプロビジョニングファイルをユーザーに提供して、Receiverを自動的に構成できるようにします。 Receiverをインストールした後で、提供されたファイルをユーザーが開くとReceiverが自動的に構成されます。 Receiver for Webサイトを構成する場合は、そのサイトからユーザーにReceiverのプロビジョニングファイルを提供することもできます。
  詳しくは、StoreFrontのドキュメントの「ユーザーに配布するストアプロビジョニングファイルをエクスポートするには」を参照してください。

アカウント情報をユーザーに手入力させる

ユーザーが手動でアカウントをセットアップできるようするには、ユーザーが仮想デスクトップとアプリケーションへ接続するために必要とする情報を提供します。

- StoreFrontストアへの接続の場合は、そのサーバーのURLを提供します。 例：https://servername.company.com
  Web Interface展開環境の場合は、XenApp ServicesサイトのURLを提供します。

- NetScaler Gatewayを介する接続の場合は、ユーザーがすべての構成済みストアを表示する必要があるのか、または特定の
  NetScaler Gatewayに対するリモートアクセスが有効になった単一のストアだけにアクセスする必要があるのかを最初に判断します。
  - 構成済みストアをすべて表示させる場合は、ユーザーにNetScaler Gatewayの完全修飾ドメイン名を提供します。
  - 特定のストアへのアクセスに限定する場合は、ユーザーにNetScaler Gatewayの完全修飾ドメイン名とストア名を次の形式で提供します。
    NetScalerGatewayFQDN?MyStoreName

    たとえば、"SalesApps"という名前のストアがserver1.comへのリモートアクセスが有効で、"HRApps"と言う名前のストアがserver2.comへのリモートアクセスが有効な場合、ユーザーはSalesAppsにアクセスするには、HRAppsにアクセスするにはと入力する必要があります。 この機能では、新規ユーザーはURLを入力してアカウントを作成する必要があり、電子メールベースの検出は使用できません。

ユーザーが新しいアカウントの詳細を入力すると、Receiverにより接続が検証されます。 検証に成功すると、そのアカウントにログオンするための画面が開きます。

Receiverユーザーがアカウントを管理するには、Receiverのホームページで▾をクリックし、**[アカウント]**を選択します。

複数のストアアカウントの自動的共有

複数のストアアカウントがある場合は、セッションの確立時にCitrix Receiver for Windowsを構成してすべてのアカウントに自動的に接続できます。 Receiverを開く時にすべてのアカウントを自動的に表示するには

32ビットシステムの場合、"CurrentAccount"というキーを作成します：

場所：HKLM\Software\Citrix\Dazzle

キー名：CurrentAccount

値：AllAccount

種類：REG_SZ

64ビットシステムの場合、"CurrentAccount"というキーを作成します：

場所：HKLM\Software\Wow6432Node\Citrix\Dazzle

キー名：CurrentAccount

値：AllAccount

種類：REG_SZ

> **警告**
>
> レジストリエディタの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

Citrix Receiver環境の最適化

Oct 31, 2016

管理者は、ユーザーが効率的に作業できるようにReceiver環境を最適化できます。

- アプリケーションの起動時間の短縮
- クライアント側デバイスのマッピング
- DNS名前解決をサポートする
- プロキシサーバーを介したXenDesktop接続をサポートする
- NDSユーザーのサポートを提供する
- ReceiverでXenApp for UNIXをサポートする
- 匿名アプリケーションへのアクセスを有効にする

そのほかの最適化オプションについては、XenDesktopのドキュメントの「セッションの継続性の維持」および「HDXによるユーザーエクスペリエンスの最適化」に関するトピックを参照してください。

アプリケーションの起動時間の短縮

Feb 02, 2016

セッションの事前起動機能を使用すると、通常時および高トラフィック負荷時のアプリケーションの起動時間が短縮され、ユーザーエクスペリエンスが向上します。 事前起動機能により、ユーザーがReceiverにログオンするとき、またはログオン済みの場合は予定された時間に事前起動セッションを作成できます。

この事前起動セッションにより、最初のアプリケーションの起動時間が短縮されます。 ユーザーがReceiverで新しいアカウント接続を追加した後、次回のセッションまで事前起動セッションは適用されません。 このセッションでは、デフォルトのアプリケーションctxprelaunch.exeが実行されます。ただし、このアプリケーションはユーザーには表示されません。

セッションの事前起動機能は、StoreFront環境ではStoreFront 2.0リリース以降でサポートされます。 Web Interface環境では、ログオン用の画面が表示されるのを防ぐため、Web Interfaceの［パスワードを保存］オプションを有効にする必要があります。 セッションの事前起動機能は、XenDesktop 7環境ではサポートされません。

セッションの事前起動機能はデフォルトでは無効になっています。 この機能を有効にするには、Receiverのコマンドラインで ENABLEPRELAUNCH=trueパラメーターを指定するか、レジストリキーEnablePreLaunchにtrueを設定します。 デフォルト値（null）は、事前起動が無効であることを示します。

注：ドメインパススルー（SSON）認証をサポートするようにクライアントマシンが構成されている場合、事前起動機能が自動的に有効になります。 事前起動なしでドメインパススルー（SSON）を使用する場合は、EnablePreLaunchレジストリキーの値をfalseに設定します。
注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。
レジストリの場所は以下のとおりです。

HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle

HKEY_CURRENT_USER\Software\Citrix\Dazzle

事前起動には2つの種類があります。

- **即時事前起動**。 トラフィック量にかかわらず、ユーザーの資格情報が認証されるとすぐに事前起動が開始されます。 この設定は、通常のトラフィック負荷時に使用します。 ユーザーは、Receiverを再起動することで事前起動セッションを起動できます。
- **予定事前起動**。 予定した時間に事前起動が開始されます。 予定事前起動は、ユーザーデバイスが実行中で認証済みの場合にのみ開始されます。 これら2つの条件が満たされない場合は、予定された事前起動時間になってもセッションが起動しません。 ネットワークとサーバーの負荷を分散するため、セッションは予定された時刻を含む一定期間内に起動します。 たとえば、事前起動が午後1時45分に予定されている場合は、セッションが実際に起動するのは午後1時15分から 午後1時45分の間です。 この設定は、トラフィックの負荷が高いときに使用します。

XenAppサーバーでの事前起動の構成には、事前起動アプリケーションの作成、変更、または削除と、事前起動アプリケーションを制御するユーザーポリシー設定の更新が含まれます。 XenAppサーバー上でセッションの事前起動を構成する方法については、XenAppのドキュメントの「アプリケーションを事前起動するには」を参照してください。

icaclient.admファイルで事前起動機能をカスタマイズすることはできません。 ただし、Receiverのインストール時またはインストール後にレジストリ値を変更することで、事前起動構成を変更することができます。 3つのHKEY_LOCAL_MACHINE値と2つのHKEY_CURRENT_USER値を使用します。

- HKEY_LOCAL_MACHINE値は、Receiverのインストール時に追加されます。
- HKEY_CURRENT_USER値では、同一マシン上の特定ユーザーにHKEY_LOCAL_MACHINEとは異なる値を設定できます。 ユーザーは、管理者権限がなくてもHKEY_CURRENT_USER値を変更できます。 管理者は、この機能を設定するためのスクリプトをユーザーに提供できます。

HKEY_LOCAL_MACHINE値

Windows Server 7および8の64ビット：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

そのほかのすべての32ビットWindowsオペレーティングシステム：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch

値の名前：UserOverride

値のデータ：

0 - HKEY_CURRENT_USERの値が存在しても、HKEY_LOCAL_MACHINEの値を使用します。

1 - 存在する場合はHKEY_CURRENT_USERの値を使用します。そうでない場合は、HKEY_LOCAL_MACHINEの値を使用します。

値の名前：State

値のデータ：

0 - 事前起動を無効にします。

1 - 即時事前起動を有効にします （ユーザーの資格情報が認証されると事前起動が開始されます）。

2 - 予定事前起動を有効にします (Schedule値に指定した時刻に事前起動が開始されます)。

値の名前：Schedule

値のデータ：

予定事前起動を開始する、24時間形式の時刻と曜日です。入力形式は次のとおりです。

HH:MM|M:T:W:TH:F:S:SU - ここで、HHは時、MMは分です。 M:T:W:TH:F:S:SUは曜日です。 月曜日、水曜日、および金曜日の午後1時45分に予定事前起動を有効にするには、Schedule=13:45|1:0:1:0:1:0:0と設定します。 セッションが実際に起動するのは午後1時15分から 午後1時45分の間です。

HKEY_CURRENT_USER値

HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

値については、HKEY_LOCAL_MACHINEと同じStateおよびSchedule値を使用します。

クライアント側デバイスのマッピング

Feb 02, 2016

Receiverでは、クライアント側デバイスのマッピング（割り当て）機能がサポートされており、ユーザーはセッション内でローカルのデバイスを使用できます。 次のことを実行できます。

- ローカルのディスクドライブ、プリンター、およびCOMポートにセッションから透過的にアクセスする。
- セッションとローカルのWindowsクリップボードの間で、データをコピーして貼り付ける。
- セッション内で、サーバー上のサウンドを再生する。

Receiverでサーバーにログオンすると、使用できるクライアントドライブ、COMポート、LPTポートなどがサーバーに通知されます。 デフォルトでは、クライアントドライブがサーバーのドライブ文字にマップされ、クライアントプリンターの印刷キューがサーバー上に作成されます。このため、これらのデバイスがサーバーに直接接続されているかのように見えます。マップされたクライアント側デバイスは、そのセッションを実行中のユーザーだけが使用できます。 ユーザーがログオフするとマッピングが削除され、そのユーザーが次にログオンしたときに再び作成されます。

ログオン時に特定のデバイスが自動的にマップされないように設定するには、ポリシーのリダイレクト設定を使用します。詳しくは、XenDesktopまたはXenAppのドキュメントを参照してください。

デバイスマッピングを無効にする

Windowsのサーバーマネージャーを使用して、クライアント側デバイスのマッピングオプション（ドライブ、プリンター、ポートなど）を構成できます。 指定できるオプションについて詳しくは、リモートデスクトップサービスのドキュメントを参照してください。

クライアントフォルダーのリダイレクト

クライアントフォルダーのリダイレクトは、クライアント側のファイルがホスト側のセッションのへアクセスする方法を変更します。 サーバー上でクライアント側ドライブのマッピングのみを有効にすると、クライアントの側の全ボリュームがUNC（Universal Naming Convention）リンクとしてセッションに自動的にマップされます。 管理者がサーバー上でクライアントフォルダーのリダイレクトを有効にして、ユーザーがそれをユーザーデバイス上で構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

セッション内では、ユーザーデバイス上のすべてのファイルシステムの代わりにユーザー指定のフォルダーのみがUNCリンクとして表示されます。 レジストリでUNCリンクを無効にすると、クライアントフォルダーはマップされたドライブとしてセッション内で表示されます。 構成方法など、クライアントフォルダーのリダイレクトについて詳しくはXenDesktop 7のドキュメントを参照してください。

クライアントドライブをホスト側のドライブ文字にマップする

クライアント側ドライブのマッピング機能により、ホスト側のドライブ文字をユーザーデバイス上のドライブとしてリダイレクトできます。 たとえば、Citrixユーザーセッション内で表示されるHドライブにアクセスしたときに、ユーザーデバイスのCドライブにリダイレクトされるように設定できます。

クライアント側ドライブのマッピングは、Citrixの標準デバイスリダイレクト機能に透過的に組み込まれています。 この方法でマップされたドライブ文字は、通常のネットワークドライブのマッピングの場合と同様に、ファイルマネージャー、エクスプローラー、およびアプリケーションで使用することができます。

仮想デスクトップやアプリケーションをホストするサーバーにXenDesktopまたはXenAppをインストールするときに、クライアントドライブが自動的にマップされるサーバーのドライブ文字のセットを設定できます。 デフォルトでは、インストール

時に、個々のハードディスクおよびCDドライブに1文字ずつ、Vからのアルファベットで未使用のドライブ文字がマップされます （クライアントのフロッピーディスクドライブには、元のドライブ文字がそのままマップされます）。この場合、セッションでのドライブマッピングは、次のようになります。

クライアントドライブ文字	セッション内でアクセスするときのドライブ文字
A	A
B	B
C	V
D	U

サーバーの既存のドライブ文字をアルファベットの後ろの方の文字に変更しておくと、サーバー側のドライブ文字がクライアント側のものと競合しなくなるため、ユーザーはローカルドライブと同じドライブ文字をセッション内で使用できます。 たえば、サーバーのCドライブをMに変更し、DをNに変更しておくと、クライアントデバイスの既存のCドライブやDドライブにそのままアクセスできます。 この場合、セッションでのドライブマッピングは、次のようになります。

クライアントドライブ文字	セッション内でアクセスするときのドライブ文字
A	A
B	B
C	C
D	D

サーバーのCドライブを置き換えるために使用するドライブ文字は、インストール時に定義できます。 そのほかの固定ドライブおよびCD/DVDドライブのドライブ文字は、連続するドライブ文字に置き換えられます。たとえば、CドライブはM、DはN、EはOに置き換えられます。 これらのドライブ文字が、既存のネットワークドライブのマッピングと競合しないようにしてください。 ネットワークドライブにマップされたドライブ文字がサーバーのドライブ文字と競合する場合、ネットワークドライブのマッピングが無効になります。

クライアント側デバイスの自動マッピングを無効にしない限り、ユーザーデバイスでサーバーに再接続すると、マッピングが再確立されます。 デフォルトでは、クライアント側ドライブのマッピングが有効になっています。 設定を変更するには、リモートデスクトップ（ターミナルサービス）構成ツールを使用します。 また、ポリシーを使用して、クライアント側デバイスのマッピングを詳細に制御できます。 ポリシーについて詳しくは、eDocsでXenDesktopまたはXenAppのドキュメントを参照してください。

HDX Plug-n-Play USBデバイスリダイレクト

Updated: 2015-01-27

HDX Plug-n-PlayのUSBデバイスリダイレクトにより、カメラ、スキャナー、メディアプレーヤー、およびPOS端末など、ユーザー側のさまざまなデバイスをサーバーに動的にリダイレクトできます。 管理者やユーザーは、すべてまたは一部のデバイスのリダイレクトを制限できます。 サーバー上でポリシーを編集するかユーザーデバイス上でグループポリシーを適用して、リダイレクト設定を構成します。 詳しくは、XenAppおよびXenDesktopドキュメントの「USBとクライアント側ドライブの考慮事項」を参照してください。

重要：サーバーポリシーでこのUSBデバイスリダイレクトを禁止すると、ユーザー側でこの機能を有効にすることはできなくなります。
ユーザーは、デバイス接続時にそのデバイスのリダイレクトを許可したり、拒否したり、または毎回確認のメッセージを表示したりできます。この設定は、Receiverで行います。 この設定は新しく接続するデバイスにのみ適用され、接続済みのデバイスには適用されません。

クライアントのCOMポートをサーバーのCOMポートにマップするには

クライアント側COMポートのマッピングを有効にすると、セッション内でローカルマシンのCOMポート上のデバイスにアクセスできるようになります。 マップされたクライアントのCOMポートは、ほかのネットワークドライブのマッピングと同様の方法で使用できます。

コマンドプロンプトからクライアントCOMポートをマップできます。 また、Windowsの管理ツールのリモートデスクトップ（ターミナルサービス）構成ツールまたはポリシーを使用して、クライアントCOMポートのマッピングを制御することもできます。 ポリシーについて詳しくは、XenDesktopまたはXenAppのドキュメントを参照してください。

重要：COMポートのマッピング機能は、TAPIをサポートしません。 TAPIデバイスをクライアントのCOMポートにマップすることはできません。

1. XenDesktop 7環境で、ポリシーの [クライアントCOMポートリダイレクト] 設定を有効にします。
2. Receiverにログオンします。
3. コマンドプロンプトで、次のコマンドを実行します。

   net use com<x>: \\client\com:

   ここで、<x>にはサーバー上のCOMポート番号（ポート1～9）を指定し、<z>にはクライアントデバイス上のCOMポート番号を指定します。

4. 操作を確認するには、

   net use

   と入力しEnterキーを押します。 マップされているドライブ、LPTポート、およびマップされているCOMポートの一覧が表示されます。

   このCOMポートを仮想デスクトップやアプリケーションのセッションで使用するには、割り当てられているCOMポートにデバイスをインストールします。 たとえば、クライアントのCOM1をサーバーのCOM5にマップするには、セッション内で、COM5にCOMポートデバイスをインストールします。 この方法でマップしたCOMポートは、ユーザーデバイスのCOMポートと同じように使用できます。

DNS名前解決をサポートする

Feb 02, 2016

Citrix XML Serviceを使用してサーバーファームに接続するときに、サーバーのIPアドレスの代わりにDNS（Domain Name System：ドメインネームシステム。host.subdomain.co.jpなど）名を要求できるように、Receiverを構成できます。
重要：この機能を使用するためにDNS環境を設定していない場合は、サーバーファームでDNSアドレス解決を有効にしないことをお勧めします。
Web Interfaceを使用してリモートアプリケーションに接続するReceiverも、接続にCitrix XML Serviceを使用します。 この場合、Receiverの代わりにWeb Interfaceサーバーが DNS名を解決します。

DNSアドレス解決は、デフォルトでサーバーファームでは無効に、Receiverでは有効に設定されています。 サーバーファームでDNSアドレス解決が無効な場合、ReceiverがDNS名を要求するとIPアドレスが返されます。 ReceiverでDNSアドレス解決を無効にする必要はありません。

特定のユーザーデバイスのDNSアドレス解決を無効にするには

DNSによるサーバー名解決が使用される環境で特定のユーザーデバイスでの問題を解決するには、そのデバイスのDNS名前解決を無効にします。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. レジストリキーHKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsingに、文字列値xmlAddressResolutionTypeを追加します。
2. 値をIPv4-Portに設定します。
3. ユーザーデバイスの各ユーザーでこれを繰り返します。

プロキシサーバーを介したXenDesktop接続をサポートする

Feb 02, 2016

プロキシサーバーを使用しない環境でユーザーがWindows XP上のInternet Explorer 7.0を使用する場合は、Internet Explorerのプロキシ設定を変更する必要があります。 この場合、デフォルトでプロキシ設定が自動的に検出されます。 プロキシサーバーを使用しない環境でこのデフォルト設定を使用すると、プロキシ設定の検出時に不必要な遅延が発生します。 プロキシ設定の変更手順については、Internet Explorerのドキュメントを参照してください。 または、Web Interfaceを使ってプロキシ設定を変更できます。 詳しくは、Web Interfaceのドキュメントを参照してください。

ユーザーエクスペリエンスの向上

Feb 02, 2016

Receiverには、ユーザーエクスペリエンスを向上させるための以下の機能が用意されています。

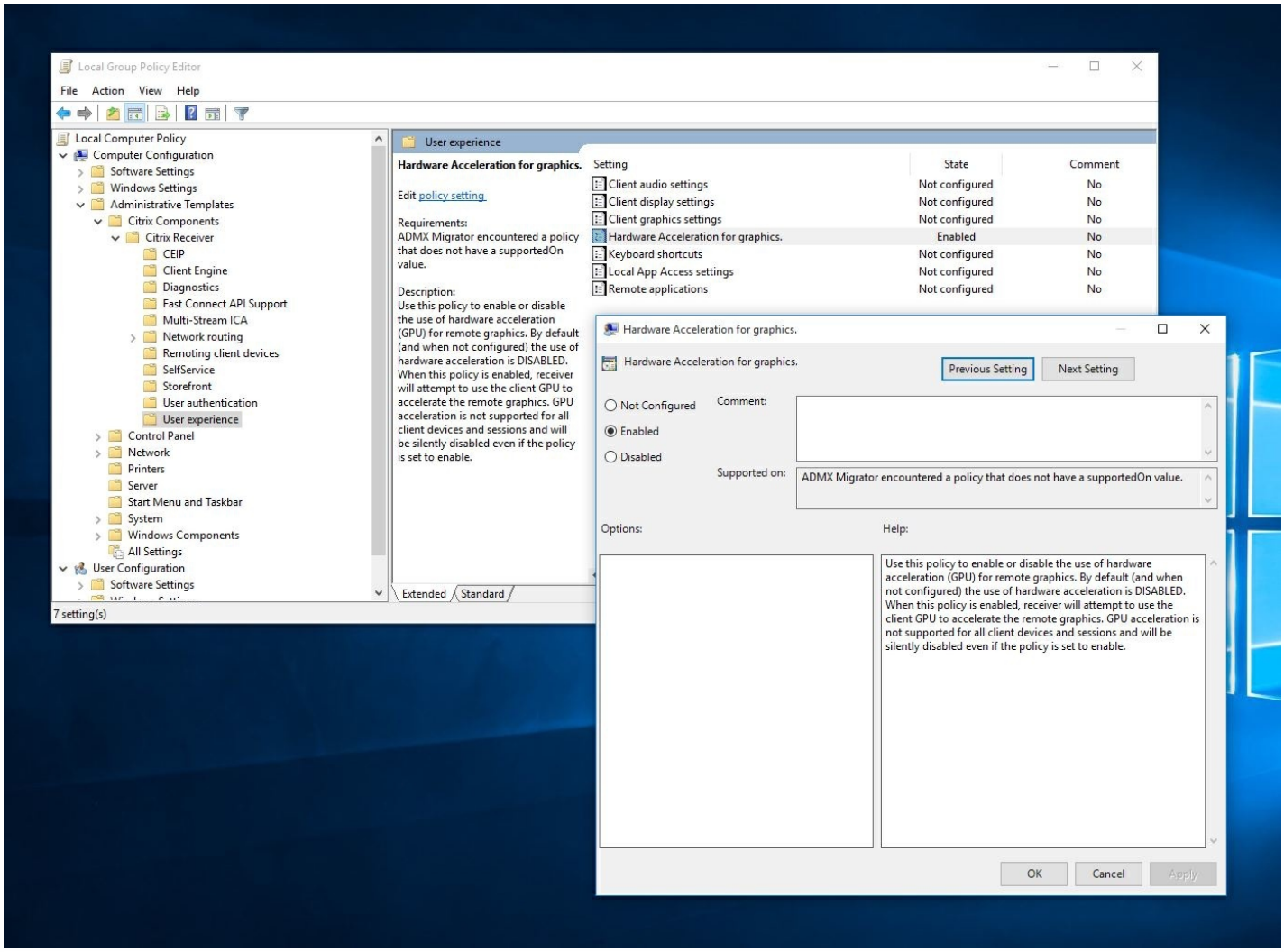
Citrix Receiver for Windowsのバージョン4.4（HDX Engine 14.4含む）を使用する場合、クライアントで利用できる場合にはいつでもH.264デコードにGPUを使用できます。 GPUデコードで使用されるAPIレイヤーはDXVA（DirectX Video Acceleration）です。

詳しくは、Improved User Experience: Hardware Decoding for Citrix Windows Receiverというブログの記事を参照してください。

> **注意**
>
> デフォルトでは、ハードウェアデコード機能はオフになっています。クライアント側のポリシーでこれを有効にできます。

ハードウェアデコードを有効にするには：

1. “receiver.adml”を“root\Citrix\ICA Client\Configuration\en”から“C:\Windows\PolicyDefinitions\en-US”にコピーします。
2. “receiver.admx”を“root\Citrix\ICA Client\Configuration”から“C:\Windows\PolicyDefinitions\”にコピーします。
3. **ローカルグループポリシーエディタ**を開きます。
4. ［コンピューターの構成］>［管理用テンプレート］>［Citrix Receiver］>［User Experience］の順に選択し、**[Hardware Acceleration for graphics]** を開きます。
5. **[有効]** をクリックして **[OK]** をクリックします。



ポリシーが適用され、ハードウェアアクセラレーションがアクティブなICAセッションで使用されているかを確認するには、次のレジストリキーを確認します。

レジストリパス：HKCU\Software\Citrix\ICA Client\CEIP\Data\GfxRender\

> ## ヒント
>
> **Graphics_GfxRender_Decoder**および**Graphics_GfxRender_Renderer**は2である必要があります。 値が1の場合、CPUベースのデコードが使用されています。

ハードウェアデコード機能が使用されている場合、次の制限事項を考慮してください。

- クライアントにGPUが２つあり、モニターの一つが２つめのGPUでアクティブな場合、CPUデコードがしよされます。
- Windows Server 2008 R2が動作するXenApp 7.xサーバーに接続する場合、ユーザーのWindowsデバイスではハードウェアデコードを使用しないことをお勧めします。 これが有効な場合、文字列を強調表示する際のパフォーマンスの低下やちらつきの問題が発生します。

Receiverは、クライアント側の複数のマイク入力をサポートします。 ユーザーは、ローカルのマイクを使用して以下の操作を実行できます。

- ソフトフォンでの通話やWeb会議などのリアルタイムのアクティビティ。
- ホストされている録音アプリケーション（ディクテーションプログラムなど）の使用。
- 録画と録音。

Receiverのユーザーは、コネクションセンターの設定を変更して、デバイスに付属しているマイクを使用するかどうか選択することができます。 XenDesktopユーザーも、［Desktop Viewer基本設定］ダイアログボックスを使用してマイクおよびWebカメラを無効にできます。

Updated: 2014-11-28

Receiverでは、最大で8つのモニターがサポートされます。

マルチモニター環境では、各モニターの製造元により解像度が異なる場合があります。 また、セッション中にモニターの解像度や向きが変更されることもあります。

セッションを複数のモニター上に表示する場合、以下の2つのモードがあります。

- 全画面モード。セッションはマルチモニター全体に表示されます。ローカルでの場合と同様に、アプリケーションウィンドウが表示領域全体に最大化されます。
  XenDesktop：Desktop Viewerウィンドウをマルチモニターのいずれかの矩形表示領域内に表示するには、隣接するモニターにかかるようにウィンドウのサイズを変更して［最大化］ボタンをクリックします。
- ウィンドウモード。単一のモニターがセッション用に使用されます。アプリケーションウィンドウは個々のモニター上に最大表示されません。

XenDesktop：同じ割り当て（デスクトップグループ）に含まれるデスクトップを続けて起動すると、ウィンドウ設定が保持され、デスクトップが同じモニターに表示されます。 矩形配置構成のマルチモニター環境では、複数の仮想デスクトップを1つのデバイス上で表示できます。 デバイスのプライマリモニターをXenDesktopセッションで使用する場合は、セッションでもそのモニターがプライマリモニターになります。 そうでない場合は、セッション内の最も小さい番号のモニターがプライマリモニターになります。

マルチモニター環境をサポートするには、次の条件を満たしている必要があります。

- ユーザーデバイスの構成でマルチモニターがサポートされている。
- ユーザーデバイスのオペレーティングシステムが各モニターを検出できる。 Windowsプラットフォームでモニターを検出できるかどうかは、［ディスプレイ］、［ディスプレイの設定の変更］の順に選択して確認します。ここで、各モニターが別々に表示されていることを確認します。
- モニターが検出された後は、次の作業を行います。
  - **XenDesktop：**Citrixコンピューターポリシーの［表示メモリの制限］設定を使用して、グラフィックメモリの制限を構成します。
  - **XenApp：**インストールしたXenAppサーバーのバージョンに応じて、次の操作を行います。
    - Citrixポリシーの［表示メモリの制限］設定を使用して、グラフィックメモリの制限を構成します。
    - XenAppサーバー用Citrix管理コンソールの左ペインでサーバーファームを選択し、タスクペインで[サーバーファームのプロパティの変更］、［すべてのプロパティの変更］、［サーバーのデフォルト設定］、［HDX Broadcast］、［表示設定］の順に選択します（または［サーバーファームのプロパティの変更］、［すべてのプロパティの変更］、［サーバーのデフォルト設定］、［ICA］、［表示設定］の順に選択します）。そして、［各セッションのグラフィックで使用する最大メモリ］を設定します。

この値を、グラフィックメモリを提供するのに十分なサイズに設定します（単位はキロバイト）。 このボックスの値が必要なサイズに満たないと、公開リソースが一部のモニター上でしか表示されません。

XenAppおよびXenDesktopのセッションのグラフィックメモリ要件の計算については、CTX116286を参照してください。

ポリシーの［ユニバーサル印刷最適化デフォルト］設定で［非管理者によるこれらの設定の変更を許可する］チェックボックスをオンにすると、ポリシーで指定されている［イメージ圧縮］および［イメージおよびフォントのキャッシュ］オプションの設定をユーザーが変更できるようになります。

ユーザーがプリンター設定を上書きするには

1. ユーザーデバイス上で、アプリケーションの［印刷］ダイアログボックスを開き、［プロパティ］をクリックします。
2. ［クライアント設定］タブで［高度な最適化］をクリックし、［イメージ圧縮］および［イメージおよびフォントキャッシュ］オプションの設定を変更します。

Windowsタブレットから仮想アプリケーションおよびデスクトップへのタッチ操作によるアクセスを有効にするため、テキスト入力フィールドがアクティブになったり、デバイスがテントまたはタブレットモードになったりすると、Receiverによって自動的にスクリーンキーボードが表示されます。

一部のデバイスおよび一部の環境下では、Receiverがデバイスのモードを正確に検出できず、必要時にスクリーンキーボードが表示されないことがあります。

変換可能なデバイス（取り外し可能なキーボード付タブレット）を使っている場合にスクリーンキーボードの表示を抑制するには、REG_DWORD値DisableKeyboardPopup in HKLM\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiverを作成し、値を1に設定します。
注：x64マシンでは、HKLM\SOFTWARE\Wow6432Node\ Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiverに値を作成します

Receiverで特定の機能を実行するキーの組み合わせを構成できます。 キーボードショートカットのポリシーが有効な場合、Citrixショートカットキーのマッピング、Windowsショートカットキーの動作、およびセッションでのキーボードの種類を指定できます。

1. 管理者として、［スタート］メニューからgpedit.mscを実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。

   注：既にicaclientテンプレートをグループポリシーオブジェクトエディターにインポートしている場合、手順2.～5.は省略できます。
2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、ReceiverのConfigurationフォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、icaclient.admを選択します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. グループポリシーエディターで、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］、［User Experience］の順に開きます。
7. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックして必要なオプションを選択します。

Receiverでは32ビットHigh Colorアイコンがサポートされ、Citrixコネクションセンターに表示されるアプリケーションのアイコンに適した色数が自動的に選択されます。シームレスアプリケーションを実行しているときに［スタート］メニューとタスクバーに表示されるアプリケーションのアイコンも、同様に処理されます。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。
色数を設定するには、レジストリキーHKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferencesに文字列のレジストリ値TWIDesiredIconColorを追加し、目的の色数を値のデータとして定義します。 定義できるアイコンの色数は、4、8、16、24、および32ビット/ピクセルです。 ネットワーク接続が低速な場合は、ユーザーはより少ない色数を選択できます。

企業組織にはそれぞれ異なるニーズがあります。 ユーザーが仮想デスクトップにアクセスする方法の要件は、ユーザーによって、そして企業ニーズが展開するにつれて変化する可能性があります。 ユーザーが仮想デスクトップに接続したり接続を構成したりするときの手順は、管理者によるReceiver for Windowsのセットアップ方法によって異なります。

ユーザーが仮想デスクトップを操作する必要がある場合は、**Desktop Viewer**を使用します。 ユーザーの仮想デスクトップは公開仮想デスクトップにすることができ、または共有デスクトップや専用デスクトップにもすることができます。 このアクセスシナリオでは、Desktop Viewerツールバー機能により、ユーザーが仮想デスクトップをローカルデスクトップ上のウィンドウ内に開いて、必要に応じて仮想デスクトップの表示領域や表示サイズを変更できます。 ユーザーは必要に応じて設定を変更でき、同じユーザーデバイス上で複数のXenDesktop接続を使用して複数の仮想デスクトップを実行できます。

注：仮想デスクトップの解像度を変更する場合は、Citrix Receiverを使用する必要があります。 Windowsコントロールパネルで解像度を変更することはできません。

Desktop Viewerセッションでは、Windowsロゴ + Lキーはローカルコンピューターに送信されます。

Ctrl + Alt + Delキーは、ローカルコンピューターに送信されます。

通常、Microsoft社のユーザー補助機能である固定キー、フィルターキー、および切り替えキー機能を有効にするキーはローカルコンピューターに送信されます。

Desktop Viewerのユーザー補助機能として、Ctrl + Alt + Breakキーを押すと、ポップアップウィンドウでDesktop Viewerツールバーが開きます。

Ctrl + Escキーは、リモートの仮想デスクトップに送信されます。

注：デフォルトでは、Desktop Viewerを最大化した場合はAlt + Tabキーを押すとセッション内のウィンドウ間でフォーカスが切り替わります。 Desktop Viewerをウィンドウ内に表示している場合は、Alt + Tabキーを押すとセッション外のウィンドウ間でフォーカスが切り替わります。
ホットキーシーケンスは、Citrixにより設計されたキーの組み合わせです。 たとえば、Ctrl + F1シーケンスはCtrl + Alt + Delキーを再現し、Shift + F2はアプリケーションの全画面モードとウィンドウモードを切り替えます。 Desktop Viewerで表示されている仮想デスクトップ（つまり、XenDesktopセッション）ではホットキーシーケンスを使用できませんが、公開アプリケーション（つまり、XenAppセッション）ではこれを使用できます。

仮想デスクトップセッション内から同じ仮想デスクトップに接続することはできません。 これを行うと、既存のデスクトップセッションが切断されます。 そのため、次のことをお勧めします。

- 管理者は、仮想デスクトップ上のクライアントが、同じデスクトップを公開しているサイトに接続するように構成しない。
- ユーザーは、同じデスクトップをホストしているサイトを参照しない（自動的に既存のセッションに再接続するようサイトが構成されている場合）。
- ユーザーは、同じデスクトップをホストしているサイトを参照したりそのデスクトップを起動したりしない。

仮想デスクトップとして動作するコンピューターにローカルでログオンするユーザーは、そのデスクトップへの接続がブロックされます。

ユーザーが仮想デスクトップ内から（XenAppで公開された）仮想アプリケーションに接続し、別の管理者がXenAppを管理している環境では、ローカルのデバイスが仮想デスクトップセッションおよび公開アプリケーションセッションで同様にマップされるように、XenApp管理者と共同してデバイスマッピングを定義することをお勧めします。 仮想デスクトップセッションではローカルドライブがネットワークドライブとして表示されるため、XenApp管理者がドライブマッピングポリシーでネットワークドライブ（リモートドライブ）のマッピングを許可する必要があります。

ユーザーがセッションを起動しているときに状態インジケーターが表示される時間を変更できます。 タイムアウト期間を変更するには、REG_DWORD値のSI INACTIVE MSをHKLM\SOFTWARE\Citrix\ICA CLIENT\Engine\で作成します。 状態インジケーターをすぐに非表示したい場合は、REG_DWORD値を4に設定します。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

接続の保護

Feb 02, 2016

環境のセキュリティを最大限に高めるには、Citrix Receiverと公開リソースの間の接続を保護する必要があります。 Citrix Receiverでは、スマートカード認証、証明書失効一覧のチェック、Kerberos認証によるパススルー認証など、さまざまな認証方法を構成できます。

Windowsコンピューターでは、Windows NTチャレンジ/レスポンス（NTLM）認証がデフォルトでサポートされています。

ドメインパススルー認証の構成

Feb 02, 2016

このトピックでは、XenDesktopまたはXenAppでCitrix Receiverのドメインパススルー認証を有効にする方法について説明します。

> ## 注意
>
> この例では、Citrix Receiverのインストール、コンピューターポリシーのアプリケーション、およびクライアントオペレーティングシステム上の信頼されているサイトの構成は手動で実行されます。 グループポリシーオブジェクト（GPO）テンプレートをいったん構築したら、それをCitrix Receiverがインストールされているいずれのドメインクライアントマシンにも適用できます。

Citrix Receiverのインストール時には、ドメインパススルー（SSON）を有効にする2通りの方法があります：

- コマンドラインインストールの使用
- グラフィカルユーザーインターフェイスの使用

コマンドラインインターフェイスを使用したドメインパススルーの有効化

コマンドラインインターフェイスを使用してドメインパススルー（SSON）を有効にするには

1. Citrix Receiver 4.xを**/includeSSON**イッチでインストールします。
   - 1つまたは複数のStoreFrontストアをインストールします（この手順は後で完了できます）。StoreFrontストアのインストールはドメインパススルー認証のセットアップに必須の条件ではありません。
   - Citrix Receiverの起動によりパススルー認証が有効となっているか確認し、Citrix Receiverがインストールされるエンドポイントの再起動後にタスクマネージャーでssonsvr.exeプロセスが実行中かを確認します。

> ## 注意
>
> 1つまたは複数のStoreFrontストアを追加するための構文については、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」を参照してください。

グラフィカルユーザーインターフェイスを使用したドメインパススルーの有効化

グラフィカルユーザーインターフェイスを使用してドメインパススルーの有効にするには

1. Citrix Receiverインストールファイル（CitrixReceiver.exe）を検索します。
2. **CitrixReceiver.exe**をダブルクリックしてインストーラーを起動します。
3. シングルサインオンの有効化インストールウィザードで、シングルサインオンを有効にするチェックボックスをオンにしてCitrix ReceiverでSSON機能を有効にしてインストールします。これは、Citrix Receiverをコマンドラインスイッチの**/includeSSON**を使ってインストールするのと同じです。

次の図は、シングルサインオンを有効にする方法を示しています。

> ## 注意
>
> シングルサインオンの有効化インストールウィザードは、ドメイン参加マシンでフレッシュインストールをする場合にのみ使用できます。

Citrix Receiverの起動によりパススルー認証が有効となっているか確認し、Citrix Receiverがインストールされるエンドポイントの再起動後にタスクマネージャーで**ssonsvr.exe**プロセスが実行中かを確認します。

このセクションの情報を使ってSSON認証用のグループポリシー設定を構成します。

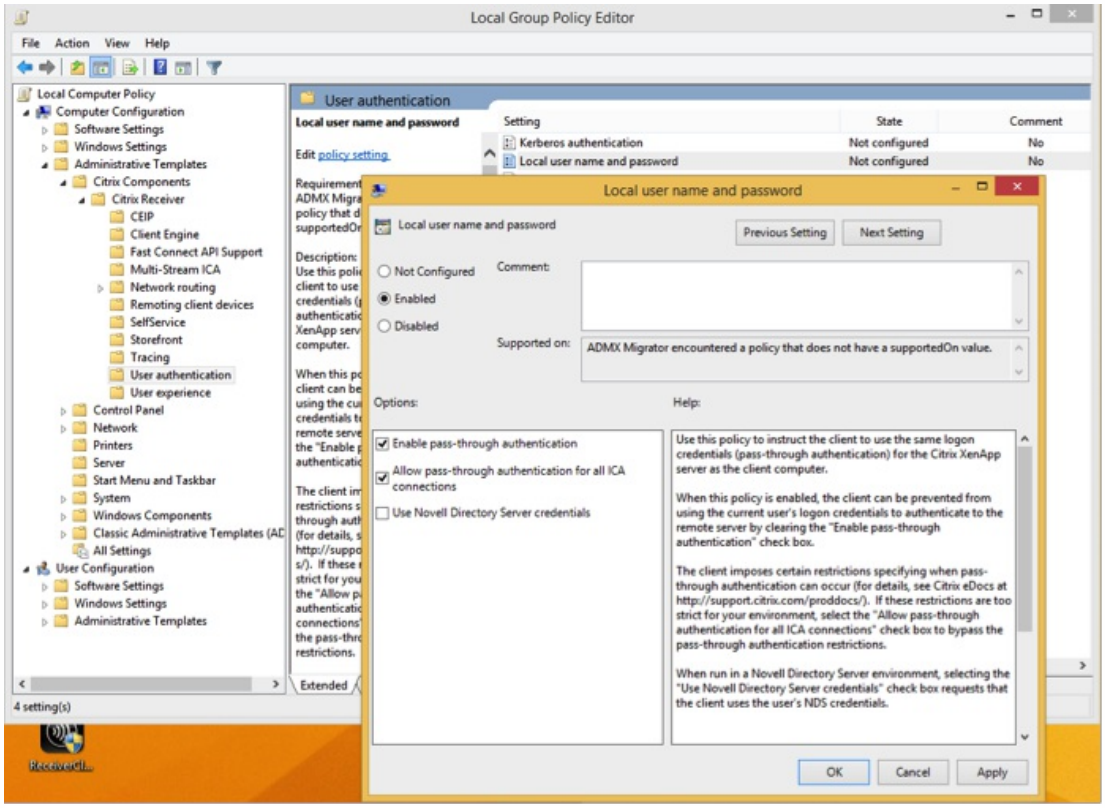
> ## 注意
>
> SSONに関連するGPOポリシー設定のデフォルト値は、**Enable pass-through authentication**で、SSONが有効になります。 次の手順でこの設定を変更します。

SSONグループポリシーに対するADMXファイルの使用

次の手順により、ADMXファイルを使ってグループポリシー設定を構成します。

1. グループポリシーファイルを読み込みます。 Citrix Receiver 4.3以降を使ったインストールでは、%SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configurationフォルダーにある**Receiver.ADMX**または**Receiver.ADML**を使用します。
2. **gpedit.msc**を開いて［**コンピューターの構成**］>［**管理テンプレート**］>［**Citrix Component**］>［**Citrix Receiver**］>［**User Authentication**］の順に選択します。
3. （ユーザーのローカルマシンまたはVDAデスクトップゴールドイメージ、あるいはその両方で）次のローカルコンピューターGPO設定を有効にします。
   - ［Local user name and password］を選択します。
   - ［**有効**］をクリックします。
   - ［**Enable pass-through authentication**］チェックボックスをオンにします。

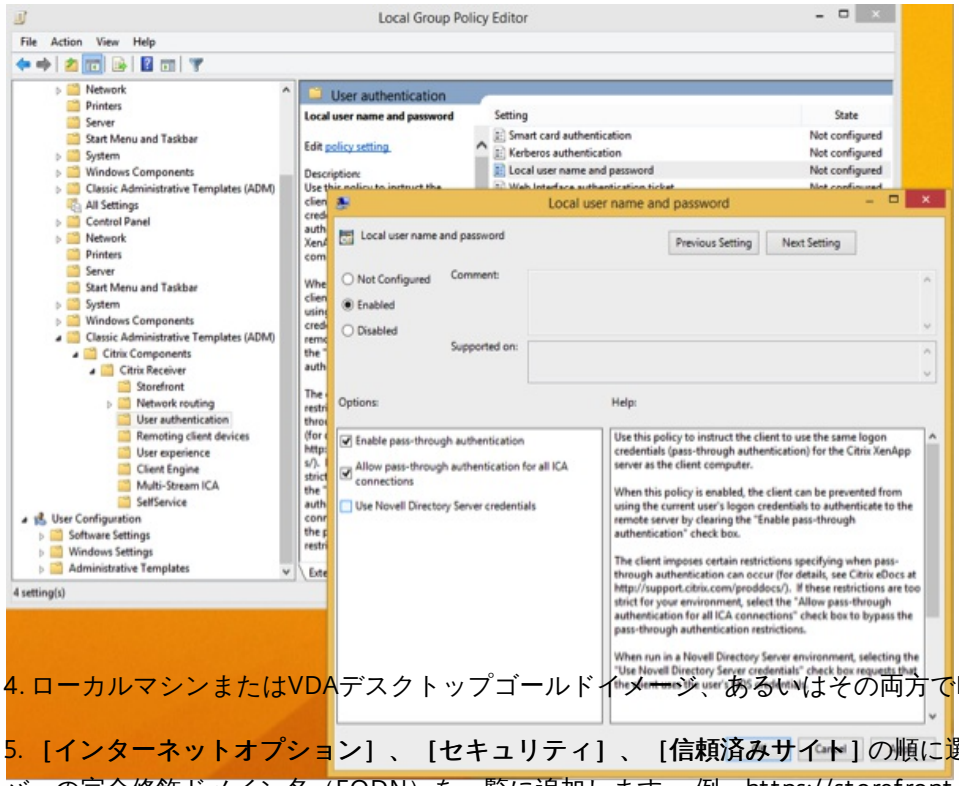
4. （Citrix Receiverがインストールされた）エンドポイントまたはVDAデスクトップゴールデンイメージを再起動します。



SSONグループポリシーに対するADMファイルの使用

次の手順により、ADMファイルを使ってグループポリシー設定を構成します。

1. **[コンピューターの構成]** > **[管理用テンプレート]** > **[テンプレートの追加と削除]** の順に選択してローカルグループポリシーエディタを開きます。
2. **[Add]** をクリックしてADMテンプレートを追加します。
3. receiver.admテンプレートを問題なく追加したら、**[コンピューターの構成]** > **[管理者テンプレート]** > **[従来の管理用テンプレート（ADM）]** > [Citrix Components] > [Citrix Receiver] > [User authentication] の順に選択します。



4. ローカルマシンまたはVDAデスクトップゴールドイメージ、あるいはその両方でInternet Explorerを開きます。

5. **[インターネットオプション]**、**[セキュリティ]**、**[信頼済みサイト]**の順に選択し、ストアパスのないStoreFrontサーバーの完全修飾ドメイン名（FQDN）を一覧に追加します。 例、https://storefront.example.com

> ## 注意
>
> またMicrosoft GPOを使って、StoreFrontサーバーを信頼済みサイトに追加することもできます。 GPOは**ゾーンの割り当て一覧へのサイト**と呼ばれ、**[コンピューターの構成]** > **[管理用テンプレート]** > **[Windowsコンポーネント]** > **[Internet Explorer]** > **[インターネットコントロールパネル]** > **[セキュリティページ]**の順に選択してアクセスできます。

6. いったんログオフしてから、再度Citrix Receiverエンドポイントにログオンします。

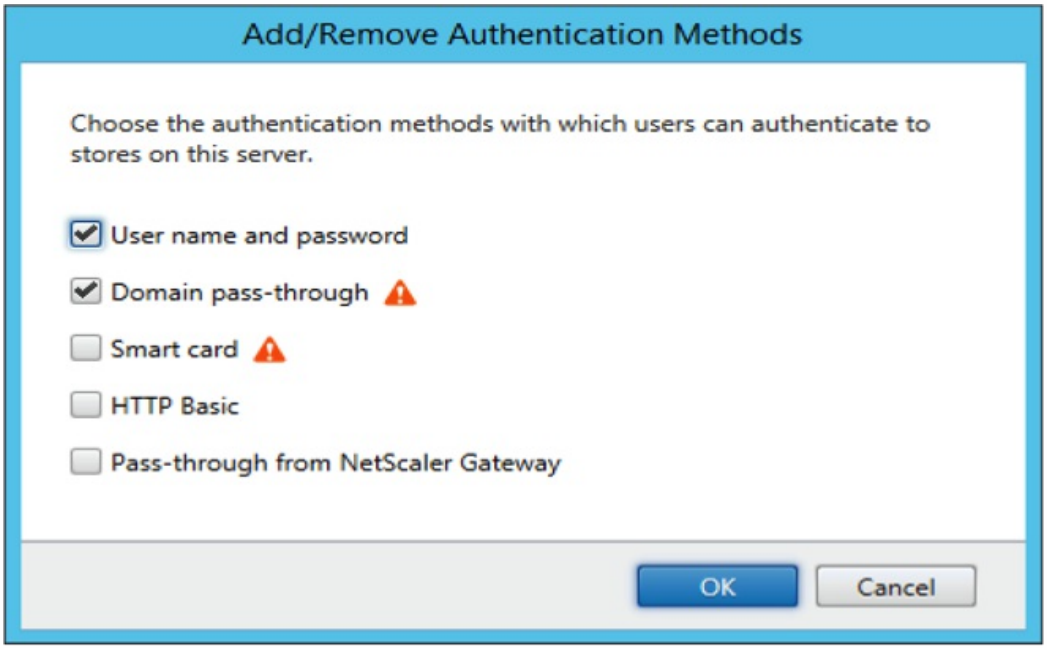
Citrix Receiverを開くと、現在のユーザーがドメインにログオンしている場合は、ユーザーの資格情報がStoreFrontにパススルーされ、ユーザーの［スタート］メニュー設定を含む、Citrix Receiver内にアプリやデスクトップが列挙されます。 ユーザーがアイコンをクリックすると、Citrix Receiverがユーザーのドメイン資格情報をDelivery Controllerにパススルーし、アプリまたはデスクトップが開きます。

次の手順により、StoreFrontおよびWeb InterfaceでSSONを構成します

1. 管理者としてDelivery Controllerにログオンします。
2. （管理者権限で）Windows PowerShellを開きます。 PowerShellを使うと、コマンドを実行してDelivery ControllerがStoreFrontから送信されるXML要求を信頼できるようにできます。
3. Citrixコマンドレットが読み込まれていない場合は、「**Add-PSSapin Citrix***」と入力して**Enter**キーを押します。
4. Enterキーを押します。
5. 「**Add-PSSnapin citrix.broker.admin.v2**」と入力して**Enter**キーを押します。
6. 「**Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True**」と入力して**Enter**キーを押します。
7. PowerShellを閉じます。

StoreFrontの構成

SSONをStoreFrontおよびWeb Interfaceで構成するには、StudioをStoreFrontサーバーで開いて **[認証]** > **[認証方法の追加と削除]** の順に選択します。 **[ドメインパススルー]** を選択します。



Web Interface構成

SSONをWeb Interfaceで構成するには、 **[Citrix Web Interface Management]** > **[XenApp Sevices Sites]** > **[Authentication Methods]** の順に選択して **[Pass-through]** を選択します

FastConnect APIはHTTP基本認証方式を採用しています。これは、ドメインパススルー、KerberosKerberos、およびIWAに割り当てられている認証方式と頻繁に混乱されます。 Citrixは、StoreFront上やICAグループポリシーではIWAを無効にすることをお勧めします。

Kerberosを使用したドメインパススルー認証の構成

Feb 02, 2016

このトピックの内容は、Citrix ReceiverとStoreFront、XenDesktop、またはXenApp間の接続にのみ適用されます。

Citrix Receiver for Windowsでは、スマートカードを使用する展開環境でのKerberosによるドメインパススルー認証がサポートされます。 Kerberosとは、統合Windows認証（IWA）に含まれる認証方法の1つです。

Kerberos認証を有効にすると、認証時にCitrix Receiverのパスワードが使用されません。このため、トロイの木馬型の攻撃でユーザーデバイス上のパスワードが漏えいすることを避けることができます。 ユーザーは、指紋照合などの生体認証も含めて、さまざまな認証方式を使用してユーザーデバイスにログオンでき、公開リソースへ接続するときに資格情報を再入力する必要もありません。

Citrix Receiver、StoreFront、XenDesktop、およびXenAppでスマートカード認証が構成されており、ユーザーがスマートカードを使用する場合、Citrix ReceiverではKerberosによるパススルー認証が以下のように処理されます。

1. Citrix Receiverのシングルサインオンサービスがスマートカードの PINを取得します。
2. Citrix Receiverは、IWA（Kerberos）を使用してStoreFrontへのユーザー認証を行います。 すると、使用可能な仮想デスクトップおよびアプリケーションの情報をStoreFrontがReceiverに提供します。
   注：この段階ではKerberos認証を使用する必要はありません。 PINの再入力が求められないようにするためだけにReceiverのKerberosを有効にします。 ReceiverでKerberos認証を使用しない場合、StoreFrontへの認証にスマートカード資格情報が使用されます。
3. HDXエンジン（従来「ICAクライアント」と呼ばれていたもの）がスマートカードのPINをXenDesktopまたはXenAppに渡します。これにより、ユーザーがWindowsセッションにログオンできます。 最後に、XenDesktopまたはXenAppが、要求されたリソースを配信します。

Citrix ReceiverでKerberos認証を使用する場合は、以下のように構成する必要があります。

- Kerberosを使用するには、サーバーとReceiverを、同じまたは信頼されているWindows Serverドメイン内に設置する必要があります。 さらに、管理タスクを割り当てられるように、［Active Directoryユーザーとコンピューター］を使ってサーバーの信頼関係を構成する必要があります。
- ドメイン、およびXenDesktopやXenAppでKerberosが有効になっている必要があります。 セキュリティを強化するには、Kerberos以外のIWAオプションを無効にして、ドメインで必ずKerberosが使用されるようにします。
- リモートデスクトップサービス接続で、基本認証や保存されたログオン情報を使用したり、常にユーザーにパスワードを入力させたりする場合、Kerberosによるログオンは使用できません。

このトピックの以降のセクションでは、一般的な環境でのドメインパススルー認証の構成方法について説明します。 カスタムの認証ソリューションを使用していたWeb Interface環境をStoreFrontに移行する場合の注意事項については、Citrixのテクニカルサポート担当者に問い合わせてください。

> ### 警告
>
> このトピックの一部の構成手順では、レジストリの編集が必要です。 レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

XenDesktop環境でのスマートカード展開について精通していない場合は、XenDesktopドキュメントの「展開環境の保護」のスマートカードに関する内容を事前に理解しておくことをお勧めします。

Citrix Receiverのインストール時に、以下のコマンドラインオプションを指定します。

- /includeSSON
  これにより、ドメインに参加しているコンピューターにシングルサインオンコンポーネントがインストールされ、ReceiveのIWA（Kerberos）によるStoreFrontへの認証が有効になります。 シングルサインオンコンポーネントは、スマートカードのPINを格納します。次に、HDXエンジンがこのPINを使用して、XenDesktopがスマートカードハードウェアと資格情報にアクセスできるようにします。 XenDesktopは、自動的にスマートカードから証明書を選択して、HDXエンジンからPINを取得します。

  関連するオプションのENABLE_SSONはデフォルトで有効になっています。これを無効にしないでください。

  何らかのセキュリティポリシーによりデバイス上でシングルサインオンを有効にすることが禁止される環境では、以下のポリシーを使用してReceiverを構成します。

  ［管理用テンプレート］> ［従来の管理用テンプレート（ADM）］> ［Citrix Components］> ［Citrix Receiver］> ［User authentication］> ［Local user name and password］

  注：このシナリオでは、HDXエンジンでKerberosではなくスマートカード認証を使用しています。このため、HDXエンジンで常にKerberosを使用するためのオプションENABLE_KERBEROS=Yesは使用しないでください。

設定を適用するには、ユーザーデバイス上のReceiverを再起動します。

StoreFrontを以下のように構成します。

- StoreFrontサーバー上のdefault.icaファイルで、DisableCtrlAltDel を falseに設定します。
  注：すべてのクライアントマシンでReceiver for Windows 4.2以降を実行している場合には、この手順は必要がありません。
- StoreFrontサーバーの認証サービスを構成するときに、［ドメインパススルー］チェックボックスをオンにします。 これにより、統合Windows認証が有効になります。 ［スマートカード］チェックボックスは、スマートカードを使用してStoreFrontに接続する非ドメイン参加のクライアントをサポートする場合のみオンにします。

StoreFrontでスマートカードを使用する場合は、StoreFrontドキュメントの「認証サービスの構成」を参照してください。

FastConnect APIはHTTP基本認証方式を採用しています。これは、ドメインパススルー、KerberosKerberos、およびIWAに割り当てられている認証方式と頻繁に混乱されます。 Citrixは、StoreFront上やICAグループポリシーではIWAを無効にすることをお勧めします。

スマートカード認証の構成

Feb 02, 2016

Receiver for Windowsでは、以下のスマートカード認証機能がサポートされます。 XenDesktopおよびStoreFrontでの構成については、これらの製品のドキュメントを参照してください。 このトピックでは、Receiver for Windowsでスマートカードを使用するための構成について説明します。

- **パススルー認証（シングルサインオン）** –ユーザーがReceiverにログオンするときに使用するスマートカードの資格情報が保持されます。 これにより、Receiverでのスマートカード認証が以下のように処理されます。
  - ドメインに属しているデバイスのユーザーがスマートカードの資格情報でReceiverにログオンした場合、仮想デスクトップやアプリケーションの起動時に格情報を再入力する必要はありません。
  - ドメインに属していないデバイスのユーザーがスマートカードの資格情報でReceiverにログオンした場合、仮想デスクトップやアプリケーションの起動時に資格情報を再入力する必要があります。

  パススルー認証を使用するには、StoreFrontおよびReceiverでの構成が必要です。

- **2モード認証** – 認証方法として、スマートカードと、ユーザー名およびパスワードの入力を選択できます。 この機能は、ユーザーがスマートカードを使用できない場合（スマートカードを自宅に忘れた場合や資格情報の有効期限が切れた場合など）に便利です。 これを実行できるようにするには、スマートカードを許可するため DisableCtrlAltDel メソッドを False に設定して、サイトごとに専用ストアをセットアップする必要があります。 2モード認証にはStoreFront構成が必要です。 NetScaler Gatewayが解決策にある場合、構成する必要もあります。
  また2モード認証により、StoreFront管理者はStoreFrontコンソールで選択して同じストアにエンドユーザーにユーザー名とパスワードの両方とスマートカード認証を提供できます。 StoreFrontのドキュメントを参照してください。

- **複数の証明書** – 単一または複数のスマートカードを使用する場合、複数の証明書を使用できます。 ユーザーがスマートカードをリーダーに挿入すると、ユーザーデバイス上で実行する、Receiverを含むすべてのアプリケーションで複数の証明書を使用できるようになります。 証明書の選択方法を変更するには、Receiverを構成します。
- **クライアント証明書による認証** – この機能を使用するには、NetScaler Gateway/Access GatewayおよびStoreFrontでの構成が必要です。
  - NetScaler Gateway/Access Gatewayを使ってStoreFrontリソースにアクセスする場合、ユーザーがスマートカードを取り外した後で再認証が必要になることがあります。
  - NetScaler Gateway/Access GatewayのSSL構成で常にクライアント証明書による認証が使用されるようにすると、より安全になります。 ただし、この構成では2モード認証を使用できません。
- **ダブルホップセッション** – ダブルホップセッションでは、Receiverとユーザーの仮想デスクトップとの間に追加の接続が確立されます。 ダブルホップセッションをサポートする展開方法については、XenDesktopのドキュメントを参照してください。
- **スマートカード対応のアプリケーション** – Microsoft OutlookやMicrosoft Officeなどのスマートカード対応アプリケーションでは、仮想デスクトップやアプリケーションセッションでドキュメントにデジタル署名を追加したりファイルを暗号化したりできます。

前提条件

このトピックの内容を理解するには、XenDesktopおよびStoreFrontのドキュメントで説明されているスマートカードについての理解が必要です。

制限事項

- 証明書は、ユーザーデバイス上ではなくスマートカード上に格納されている必要があります。
- Receiver for Windowsはユーザー証明書を保存しませんが、構成時にPINを格納できます。 PINはユーザーセッションの間

に非ページ化メモリにのみキャッシュされ、ディスク内にはどの時点においても格納されません。
- Receiver for Windowsでは、スマートカードが挿入されたときに自動的には切断セッションに再接続されません。
- スマートカード認証が構成されている場合、Receiver for Windowsでは仮想プライベートネットワーク（VPN：Virtual Private Network）のシングルサインオンやセッションの事前起動がサポートされません。 スマートカード認証でVPNトンネルを使用するには、ユーザーがNetScaler Gateway Plug-inをインストールしてWebページ経由でログオンする必要があります。この場合、各手順でスマートカードとPINによる認証が必要になります。 スマートカードユーザーは、NetScaler Gateway Plug-inを使用したStoreFrontへのパススルー認証を使用できません。
- Receiver for Windows Updaterとcitrix.comやMerchandising Server間の通信では、NetScaler Gateway上のスマートカード認証を使用できません。

> **警告**
>
> このトピックの一部の構成手順では、レジストリの編集が必要です。 レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

Receiverのインストール時に、以下のコマンドラインオプションを指定します。

- ENABLE_SSON=Yes
  シングルサインオンは、「パススルー認証」と呼ばれることもあります。 このオプションを指定すると、ReceiverでPINを繰り返し入力する必要がなくなります。

または、以下のポリシーおよびレジストリを設定します。

- ［管理用テンプレート］>［従来の管理用テンプレート（ADM）］>［Citrix Components］>［Citrix Receiver］>［User authentication］>［Local user name and password］
- シングルサインオンコンポーネントをインストールしていないデバイス上で、以下のいずれかのレジストリキーでSSONCheckEnabled から false に設定します。 これにより、ReceiverのAuthentication Managerでシングルサインオンコンポーネントがチェックされなくなり、ReceiverでStoreFrontへの認証が可能になります。
  HKEY_CURRENT_USER\Software\Citrix\AuthManager\protocols\integratedwindows\

  HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\

または、Kerberosの代わりにStorefrontに対してスマートカード認証を有効にできます。 Kerberosの代わりにStorefrontに対してスマートカード認証を有効にするには、次のコマンドラインオプションでReceiverをインストールします。 これには管理者権限が必要です。 マシンをドメインに参加させる必要はありません。

- /includeSSON を指定すると、シングルサインオン認証（パススルー認証）がインストールされます。 資格情報のキャッシュおよびパススルードメインベース認証の使用を有効にします。
- Receiverのスマートカード認証とは別の方法（ユーザー名とパスワードなど）でユーザーがエンドポイントにログオンしている場合、コマンドラインは次のようになります。
  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
  これによりログオン時に資格情報がキャプチャされるのを防ぎ、Receiverへのログオン時にPINを格納することができます。

- グループポリシーエディターで、［コンピューターの構成］、［管理用テンプレート］、［従来の管理用テンプレート

（ADM）］、［Citrix Components］、［Citrix Receiver］、［User authentication］、［Local user name and password］の順に選択します。
Enable pass-through authentication。 構成およびセキュリティ設定によっては、パススルー認証を実行するために［Allow pass-through authentication for all ICA］チェックボックスをオンにする必要があります。

StoreFrontを以下のように構成します。

- 認証サービスを構成する場合、［Smart card］チェックボックスをオンにします。

StoreFrontでスマートカードを使用する場合は、StoreFrontドキュメントの「認証サービスの構成」を参照してください。

1. デバイスのキーストアに、証明機関のルート証明書をインポートします。
2. ベンダーが提供する暗号化ミドルウェアをインストールします。
3. Receiver for Windowsのインストールと構成

複数の証明書が有効な場合、デフォルトでそれらの証明書の一覧が表示され、ユーザーは使用する証明書を選択できます。管理者は、デフォルトの証明書（スマートカードプロバイダー指定の証明書）が使用されるようにしたり、長い有効期限が残っているものが使用されるようにしたりできます。 有効なログオン証明書がない場合はユーザーにメッセージが表示され、使用可能なほかのログオン方法が提示されます。

有効な証明書とは、以下のものを指します。

- ローカルコンピューターの現在時刻に基づき、証明書が有効期限内である。
- サブジェクトの公開キーでRSAアルゴリズムが使用されており、キーの長さが1024、2048、または4096ビットである。
- Key UsageフィールドにDigital Signatureが含まれている。
- Subject Alternative Nameフィールドにユーザープリンシパル名（UPN）が含まれている。
- Enhanced Key UsageフィールドにSmart Card LogonおよびClient Authentication、またはAll Key Usagesが含まれている。
- 証明書の発行者チェーンに含まれる証明機関の1つが、TLSハンドシェイク時にサーバーから送信される、許可される識別名（DN）の1つに合致している。

証明書の選択方法を変更するには、以下のいずれかの構成を行います。

- Receiverのコマンドラインで、AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }オプションを指定する。
  デフォルト値は、Promptです。 SmartCardDefaultまたはLatestExpiryを指定して複数の証明書が該当する場合は、ユーザーが証明書を選択するための一覧が表示されます。

- レジストリキーHKEY_CURRENT_USERまたはHKEY_LOCAL_MACHINEのSoftware\[Wow6432Node\]Citrix\AuthManagerのCertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }を設定する。
  最適な証明書をユーザーが選択できるように、HKEY_CURRENT_USERでの設定は、HKEY_LOCAL_MACHINEの設定よりも優先されます。

デフォルトでは、スマートカードのCryptographic Service Provider（CSP）ではなくReceiverによりPIN入力用のメッセージが表示されます。 PINの入力が必要な場合、Receiverがメッセージを表示して、ユーザーにより入力されたPINをスマートカードのCSPに渡します。 環境やスマートカードでより厳格なセキュリティが求められる場合は、CSPコンポーネントを使用して

PIN入力用のメッセージを表示してPINを処理できます。

PIN入力の処理方法を変更するには、以下のいずれかの構成を行います。

- Receiverのコマンドラインで、AM_SMARTCARDPINENTRY=CSPオプションを指定する。
- レジストリキーHKLM\Software\[Wow6432Node\]Citrix\AuthManagerのSmartCardPINEntry=CSPを設定する。

証明書失効一覧のチェック機能の有効化

Feb 02, 2016

証明書失効一覧（CRL）のチェック機能を有効にすると、サーバー証明書が失効していないかどうかがReceiverによってチェックされます。 強制的にこのチェックを行うことにより、TLSサーバーの暗号化認証機能が強化され、ユーザーデバイスとサーバー間のTLS接続のセキュリティが向上します。

証明書失効一覧のチェック機能には、いくつかの設定レベルが用意されています。 たとえば、ローカルの証明書失効一覧だけがチェックされるようにCitrix Receiverを構成したり、ローカルおよびネットワーク上の証明書失効一覧がチェックされるように構成したりできます。 さらに、すべての証明書失効一覧で証明書の有効性が検証されたときのみログオンするように構成できます。

ローカルのコンピューターにこの変更を適用する場合は、実行中のReceiverを終了してください。 コネクションセンターを含むすべてのCitrix Receiverコンポーネントが閉じていることを確認してください。

1. 管理者として、［スタート］メニューからgpedit.mscを実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。
   注：既にicaclientテンプレートをグループポリシーオブジェクトエディターにインポートしている場合、手順2.～5.は省略できます。
2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、ReceiverのConfigurationフォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、icaclient.admを選択します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. グループポリシーエディターで、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］の順に選択します。
7. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックします。
8. ［CRL verification］の一覧からオプションを一つ選択します。
   - 無効。 証明書失効一覧をチェックしません。
   - Only check locally stored CRLs： 以前インストールまたはダウンロードされたCRLが証明書の検証に使用されます。 証明書が失効していると接続に失敗します。
   - Require CRLs for connection： CRLはローカルで、およびネットワーク上の関連の証明書発行機関からチェックされます。 証明書が失効しているか見つからないと接続に失敗します。
   - Retrieve CRLs from network： CRLは関連の証明書発行機関からチェックされます。 証明書が失効していると接続に失敗します。

   ［CRL verification］を設定しない場合、デフォルトは［Only check locally stored CRLs］となります。

Receiver通信のセキュリティ保護

Feb 02, 2016

XenDesktopサイトやXenAppファームとCitrix Receiver間の通信を保護するには、以下の一連のセキュリティ技術を使用します。

- Citrix NetScaler Gateway（Access Gateway）。 詳しくは、このセクションのトピックと、NetScaler GatewayおよびStoreFrontのドキュメントを参照してください。
  注：StoreFrontサーバーとユーザーデバイス間の通信を保護するには、NetScaler Gatewayを使用することをお勧めします。
- ファイアウォール。 ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。 サーバーの内部IPアドレスを外部インターネットアドレスにマップするネットワークファイアウォール（つまりNAT（Network Address Translation：ネットワークアドレス変換））を介してReceiverを使用する場合は、外部アドレスを構成します。
- 信頼するサーバーの構成。
- XenAppまたはWeb Interface環境では、SOCKSプロキシサーバーまたはSecureプロキシサーバー（「セキュリティプロキシサーバー」、「HTTPSプロキシサーバー」とも呼ばれます）。 プロキシサーバーでネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、Receiverとサーバー間の接続を制御できます。 Receiverは、SOCKSプロトコルとSecureプロキシプロトコルをサポートしています。
- XenAppまたはWeb Interface展開環境では、TLS（Transport Layer Security）プロトコルを使用するCitrix SSL Relay（XenDesktop 7、XenDesktop 7.1、XenDesktop 7.5、またはXenApp 7.5には適用されません）。
- XenApp 7.6およびXenDesktop 7.6の場合、ユーザーとVDA間で直接SSL接続を有効にできます （XenApp 7.6またはXenDesktop 7.6に対するSSL構成については、「SSL」を参照してください）。

Citrix Receiverは、Microsoft社のセキュリティ特化 - 機能制限（SSLF）デスクトップセキュリティテンプレートが使用されている環境と互換性があります。 これらのテンプレートは、さまざまなWindowsプラットフォームでサポートされています。 詳しくは、Microsoft社のWebサイト（http://technet.microsoft.com）で公開されている、Windowsの『セキュリティガイド』を参照してください。

NetScaler Gatewayによる接続

Feb 02, 2016

リモートのユーザーがNetScaler Gatewayを介して接続できるようにするには、StoreFrontと通信するようにNetScaler Gatewayを構成します。

- StoreFront環境では、NetScaler GatewayとStoreFrontを統合することで内部ユーザーやリモートユーザーがStoreFrontに接続できるようにします。 ユーザーは、StoreFrontに接続して仮想デスクトップおよびアプリケーションにアクセスします。 ユーザーは、Receiverを使用して接続を行います。

> **注意**
>
> NetScaler Gateway End Point Analysis Plugin（EPA）はネイティブのWindows Receiverをサポートしません。

接続の構成方法については、Citrix eDocsの「Integrating NetScaler Gateway with XenMobile App Edition」の各トピックを参照してください。 Receiver for Windowsでの設定については、以下のトピックを参照してください。

- Configuring Session Policies and Profiles for XenMobile App Edition
- Creating the Session Profile for Receiver for XenMobile App Edition
- Configuring Custom Clientless Access Policies for Receiver

リモートのユーザーがNetScaler GatewayをWeb Interface環境に接続できるようにするには、Web Interfaceと通信するようにNetScaler Gatewayを構成します。詳しくは、Citrix eDocsの「Providing Access to Published Applications and Virtual Desktops Through the Web Interface」の各トピックを参照してください。

NetScaler Gateway Enterprise Editionによる接続

Aug 30, 2016

リモートのユーザーがNetScaler Gatewayを介して接続できるようにするには、CloudGatewayのコンポーネントであるAppControllerおよびStoreFrontと通信するようにNetScaler Gatewayを構成します。

- StoreFront環境では、Access GatewayとStoreFrontを統合することで内部ユーザーやリモートユーザーがStoreFrontに接続できるようにします。 ユーザーは、StoreFrontに接続して仮想デスクトップおよびアプリケーションにアクセスします。 ユーザーは、Receiverを使用して接続を行います。
- AppController環境では、Access GatewayとAppControllerを統合することでリモートユーザーがAppControllerに接続できるようにします。 ユーザーは、AppControllerに接続してWebアプリケーションやSaaS（Software as a Service）アプリケーションを取得し、ShareFile Enterpriseサービスで共有されているドキュメントにアクセスしたりします。 ユーザーは、ReceiverまたはNetScaler Gateway Plug-inを使用して接続を行います。

接続の構成方法については、Citrix Product Documentサイトの「Integrating NetScaler Gateway with CloudGateway」の各トピックを参照してください。 Receiver for Windowsでの設定については、以下のトピックを参照してください。

- Configuring Session Policies and Profiles for CloudGateway
- Creating the Session Profile for Receiver for CloudGateway Enterprise
- Creating the Session Profile for Receiver for CloudGateway Express
- Configuring Custom Clientless Access Policies for Receiver

リモートのユーザーがAccess Gatewayを介してWeb Interface環境に接続できるようにするには、Web Interfaceと通信するようにAccess Gatewayを構成します。詳しくは、Citrix eDocsの「Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface」の各トピックを参照してください。

Secure Gatewayによる接続

Feb 02, 2016

このトピックの内容は、Web Interface環境にのみ適用されます。

Secure Gatewayを通常モードまたはリレーモードのどちらかで使用して、Receiverとサーバーの間に保護された通信チャネルを提供できます。 Secure Gatewayを通常モードで使用していて、ユーザーがWeb Interface経由で接続する場合は、Receiverの構成は不要です。

ReceiverがSecure Gatewayサーバーと通信するときは、リモートのWeb Interfaceサーバーで構成されている設定が使用されます。 Receiverのためにプロキシサーバー設定を構成する方法については、Web Interfaceのトピックを参照してください。

Secure Gateway Proxyがセキュリティで保護されたネットワーク内のサーバーにインストールされている場合は、Secure Gateway Proxyをリレーモードで使用できます。 リレーモードについて詳しくは、Secure Gatewayのトピックを参照してください。

ただし、リレーモードで使用する場合、Secure Gatewayサーバーはプロキシサーバーとして機能するため、Receiverで次の項目を構成する必要があります。

- Secure Gatewayサーバーの完全修飾ドメイン名。
- Secure Gatewayサーバーのポート番号。 Secure Gateway, Version 2.xでは、リレーモードはサポートされていません。

完全修飾ドメイン名には、以下の3つの要素を順に指定する必要があります。

- ホスト名
- サブドメイン名
- 最上位ドメイン名

たとえば、my_computer.my_company.comは完全修飾ドメイン名です。ホスト名（my_computer）、サブドメイン名（my_company）、最上位ドメイン名（com）が順に指定されています。 一般的には、サブドメイン名と最上位ドメイン名の組み合わせ（my_company.com）をドメイン名といいます。

ファイアウォールを介した接続

Feb 02, 2016

ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。 ファイアウォールが使用されている環境では、ReceiverとWebサーバーおよびCitrix製品のサーバーとの通信がファイアウォールでブロックされないように設定する必要があります。 このためには、ユーザーデバイスとWebサーバー間のHTTPラフィック（一般に標準HTTPポート80、またはセキュアなWebサーバーを使用している場合はポート443での通信）がファイアウォールを通過できるように設定します。 また、ReceiverとCitrix製品サーバー間の通信では、ポート1494とポート2598の受信ICAトラフィックがファイアウォールを通過できるように設定します。

ファイヤウォールによるネットワークアドレス変換（NAT：Network Address Translation）を使用している場合は、Web Interfaceを使って内部アドレスから外部アドレスおよびポートへのマッピングを定義できます。 たとえば、XenAppサーバーやXenDesktopサーバーに代替アドレスが設定されていない場合は、Web InterfaceからReceiverに代替アドレスが提供されるように設定できます。 これにより、Receiverでのサーバー接続で、外部アドレスおよびポート番号が使用されるようになります。 詳しくは、Web Interfaceのドキュメントを参照してください。

信頼関係の適用

Feb 02, 2016

信頼済みサーバーの構成を使用して、Receiver接続に関連する信頼関係を識別し適用することができます。 信頼関係を設定すると、Receiver管理者とユーザーはユーザーデバイス上のデータの整合性をさらに確実に信頼することができます。また、悪意を持ったReceiver接続の使用を防止できます。

この機能を有効にすると、Receiverで信頼関係に必要な条件を指定し、サーバーとの接続を信頼するかしないかを決定できます。 たとえば、特定のアドレス（https://*.citrix.comなど）に特定の接続の種類（TLSなど）を使用して接続するReceiverは、サーバーの信頼済みゾーンに接続されます。

信頼済みサーバーの構成を有効にする場合は、接続先のサーバーがWindowsの信頼済みサイトゾーンに追加されている必要があります。 Windowsの信頼済みサイトゾーンにサーバーを追加する手順について詳しくは、Internet Explorerのオンラインヘルプを参照してください。

信頼するサーバーの構成を有効にするには

ローカルのコンピューターにこの変更を適用する場合、Citrixコネクションセンターを含むすべてのReceiverコンポーネントを終了します。

1. 管理者として、［スタート］メニューからgpedit.mscを実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。
   注：既にicaclientテンプレートをグループポリシーオブジェクトエディターにインポートしている場合、手順2.～5.は省略できます。
2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、ReceiverのConfigurationフォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、icaclient.admを選択します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. ［ユーザーの構成］の［管理用テンプレート］を展開します。
7. グループポリシーエディターで、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］、［Network Routing］、［Configure trusted server configuration］の順に選択します。
8. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックします。

昇格レベルとwfcrun32.exe

Feb 02, 2016

Windows 8、Windows 7、またはWindows Vistaを実行するデバイスでユーザーアカウント制御（UAC）が有効な場合は、wfcrun32.exeと同じ昇格/整合性レベルのプロセスのみが仮想アプリケーションを起動できます。

例1：

（昇格されていない）標準ユーザーとして実行するwfcrun32.exeを使用してアプリケーションを起動する場合は、Receiverなどほかのプロセスを標準ユーザーとして実行する必要があります。

例2：

wfcrun32.exeを昇格モードで実行する場合は、非昇格モードで動作するReceiver、コネクションセンター、およびICAクライアントオブジェクトを使用するサードパーティアプリケーションはwfcrun32.exeと通信できません。

プロキシサーバーを介したReceiver接続

Feb 02, 2016

このトピックの内容は、Web Interface環境にのみ適用されます。

プロキシサーバーは、ネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、Receiverとサーバー間の接続を制御するために使います。 Receiverは、SOCKSプロトコルとSecureプロキシプロトコルをサポートしています。

Receiverがサーバーファームと通信するときは、Receiver for WebまたはWeb Interfaceのサーバー上で構成されているプロキシサーバー設定が使用されます。 プロキシサーバーの構成については、StoreFrontまたはWeb Interfaceのドキュメントを参照してください。

また、ReceiverがWebサーバーと通信するときは、ユーザーデバイス上のデフォルトのWebブラウザーで構成したプロキシサーバーの設定が使用されます。 このため、サーバーと正しく通信できるように、事前にユーザーデバイス上のWebブラウザーでインターネット接続を設定しておく必要があります。

Secure Sockets Layer (SSL) Relayによる接続

Oct 31, 2016

このトピックの内容は、XenDesktop 7.6以降、またはXenApp 7.5にのみ適用されます。

ReceiverをCitrix SSL（Secure Sockets Layer）Relayサービスと一緒に使うことができます。 ReceiverはTLSプロトコルをサポートします。 Receiver for Windows 4.2はTLS 1.0のみをサポートします。

- TLS（Transport Layer Security）は、標準化されたSSLプロトコルの最新版です。 IETF（Internet Engineering TaskForce）が、SSLの公開標準規格の開発をNetscape Communications社から引き継いだときに、SSLという名前をTLSに変更しました。 TLSは、サーバーの認証、データの暗号化、メッセージの整合性の確認を行って、データ通信を保護します。 米国政府など、 データ通信を保護するためにTLSの使用を必須としている組織もあります。 このような組織では、さらにFIPS 140（Federal Information Processing Standard）などのテスト済み暗号化基準の使用を義務付けられる場合があります。 FIPS 140は、暗号化の情報処理規格です。

このトピックの内容は、XenDesktop 7.6以降、またはXenApp 7.5にのみ適用されます。

デフォルトではCitrix SSL RelayのリスナーポートとしてTLSで保護された通信の標準ポートであるXenAppサーバーのTCPポート443が使用されます。 Citrix SSL Relayは、TLS接続要求を受信すると、その要求を解読してからサーバーに転送します。ユーザーがTLS+HTTPSブラウズを選択した場合は、Citrix XML Serviceに転送します。

443以外のリスナーポートを構成する場合、プラグインに対して非標準のリスナーポート番号を指定する必要があります。

Citrix SSL Relayを使用すると、次の通信のセキュリティを保護できます。

- TLS機能が有効になっているクライアントとサーバー間の通信。 Citrixコネクションセンターでは、TLS暗号化を使用している接続に鍵のアイコンが付きます。
- サーバーファームのXenAppサーバーと、Web InterfaceのWebサーバーとの間の通信。

インストールを保護するためのSSL Relayの構成については、XenAppのドキュメントを参照してください。

ユーザーデバイスの要件

システム要件に加えて、次の条件を満たしている必要があります。

- 128ビット暗号化をサポートしている。
- サーバー証明書にあるCA（Certificate Authority：証明機関）の署名を認証するルート証明書がインストールされている。
- サーバー上のSSL Relayが使用するTCPポートの番号がReceiverで認識されている。
- Microsoftが推奨するすべてのService Packまたはアップグレードが適用されている。

Internet Explorerをインストールしていて、システムの暗号化レベルがわからない場合は、Microsoft社のWebサイト（http://www.microsoft.com）から128ビット暗号化が含まれているサービスパックをダウンロードしてインストールしてください。

重要：Receiverでサポートされる証明書のキーの長さは、4,096ビットまでです。 使用するルート証明書、中間証明書、およびサーバー証明書のキーの長さが4,096ビットを超えると、正しく接続できない場合があります。

1. 管理者として、［スタート］メニューからgpedit.mscを実行（単一のコンピューターにポリシーを適用する場合）する

か、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。
注：既にicaclientテンプレートをグループポリシーオブジェクトエディターにインポートしている場合、手順2.～5.は省略できます。

2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、プラグイン構成フォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、icaclient.admを選択します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. グループポリシーエディターで、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］の順に選択します。
7. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックして［Allowed SSL servers］に<server:SSL relay port number>の形式で新しいポート番号を入力します。ここで、<SSL relay port number>はリスナーポート番号を示します。ワイルドカードを使用して複数のサーバーを指定できます。 たとえば、*.Test.com:<SSL relay port number>は、指定されたポートを介するTest.comへのすべての接続と一致します。

ローカルのコンピューターにこの変更を適用する場合、Citrixコネクションセンターを含むすべてのReceiverコンポーネントを終了します。

1. 管理者として、［スタート］メニューからgpedit.mscを実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。
注：既にicaclientテンプレートをグループポリシーオブジェクトエディターに追加している場合は、手順2.～5.を省略できます。
2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、ReceiverのConfigurationフォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、icaclient.admを選択します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. グループポリシーエディターで、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］の順に選択します。
7. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックして［Allowed SSL servers］に信頼済みサーバーと新しいポート番号のコンマ区切りの一覧を「servername:SSL relay port number,servername:SSL relay port number」の形式で入力します。ここで、<SSL relay port number>はリスナーポート番号を示します。 次の例のように、特定の信頼済みSSLサーバーのコンマ区切りの一覧を指定できます。
csghq.Test.com:443,fred.Test.com:443,csghq.Test.com:444
これをappsrv.iniファイルの例に当てはめると次のようになります。[Word]
SSLProxyHost=csghq.Test.com:443

[Excel]
SSLProxyHost=csghq.Test.com:444

[Notepad]

```
SSLProxyHost=fred.Test.com:443
```

ReceiverのTLSの構成と有効化

Oct 31, 2016

このトピックの内容は、XenDesktop 7.6以降、またはXenApp 7.5にのみ適用されます。

Receiverで常にTLSが使用されるようにするには、Secure GatewayサーバーまたはCitrix SSL RelayでTLSを指定します。 詳しくは、Secure GatewayまたはCitrix SSL Relayサービスのドキュメントのトピックを参照してください。

さらに、ユーザーデバイスがすべてのシステム要件を満たしていることを確認します。

すべてのReceiver通信をTLSで暗号化するには、ユーザーデバイス、Receiver、およびWeb Interfaceサーバー（使用している場合）を構成します。 StoreFront通信の保護については、Citrix製品ドキュメントのセキュリティに関するトピックを参照してください。

TLS機能が有効になっているReceiverとサーバーファーム間の通信をTLSで保護するには、サーバー証明書の証明機関（CA）の署名を認証するためのルート証明書がユーザーデバイスにインストールされている必要があります。

Receiverでは、WindowsオペレーティングシステムでサポートされているCAをサポートしています。 これらのCAのルート証明書は、Windowsと一緒にインストールされ、Windowsのユーティリティを使用して管理されます。 これらのルート証明書は、Internet Explorerで使用されているものと同じです。

ほかのCAを使用する場合は、そのCAからルート証明書を取得して、各ユーザーデバイスにインストールする必要があります。 インストールされたルート証明書はMicrosoft Internet ExplorerとReceiverの両方で使用および信頼されます。

次の管理方法や配布方法を使用して、ルート証明書をインストールできる可能性があります。

- Internet Explorer管理者キット（IEAK）ウィザードおよびプロファイルマネージャーを使用する
- サードパーティ製の配布ツールを使用する

Windowsオペレーティングシステムでインストールされた証明書が、組織のセキュリティ条件を満たしていることを確認するか、所属する組織のCAによって発行された証明書を使用してください。

1. TLSでアプリケーション一覧を暗号化して、そのデータをReceiverとWeb Interfaceサーバー間でやり取りするには、Web Interfaceサーバーの適切な設定を構成します。 SSL/TLSのための証明書をホストする、XenAppサーバーの名前を設定する必要があります。
2. ReceiverとWeb Interfaceサーバー間でやり取りされる構成情報をセキュアHTTP（HTTPS）プロトコルで暗号化するには、サーバーのURLを「https://<servername>」の形式で入力します。 Windowsの通知領域でReceiverアイコンを右クリックし、［基本設定］を選択します。
3. ［プラグインの状態］の［Online Plug-in］のエントリを右クリックし、［サーバーの変更］を選択します。

ローカルのコンピューターにこの変更を適用する場合、Citrixコネクションセンターを含むすべてのReceiverコンポーネントを終了します。

1. 管理者として、［スタート］メニューからgpedit.mscを実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。

注：既にicaclientテンプレートをグループポリシーオブジェクトエディターにインポートしている場合、手順2.～5.は省略できます。

2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、ReceiverのConfigurationフォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、icaclient.admを選択します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. グループポリシーエディターで、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］の順に選択します。
7. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックして必要なTLS設定を選択します。
   - ［TLS version］で［TLS v1.0］または［Detect version］を選択してTLSを有効にします。［Detect version］を選択した場合、ReceiverはTLS暗号化を使用して接続します。
   - ［SSL cipher suite］で［Detect version］を選択して、Receiverが行政機関レベルおよび営利企業レベルの適切な暗号の組み合わせとネゴシエートするようにします。 行政機関レベルまたは営利企業レベルのどちらかに暗号の組み合わせを限定できます。
   - ［CRL verification］で［Require CRLs for connection］を選択して、Receiverが関連の証明書発行機関から証明書失効リスト（CRL：Certificate Revocation List）を取得するよう求めます。

ローカルのコンピューターにこの変更を適用する場合、Citrixコネクションセンターを含むすべてのReceiverコンポーネントを終了します。
FIPS 140のセキュリティ規格に準拠するには、グループポリシーテンプレートを使ってパラメーターを構成するか、Web Interfaceサーバー上のDefault.icaファイルのパラメーターを含めます。 Default.icaファイルについて詳しくは、Web Interfaceの情報を参照してください。

1. 管理者として、［スタート］メニューからgpedit.mscを実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。
   注：既にicaclientテンプレートをグループポリシーオブジェクトエディターにインポートしている場合、手順3.～5.は省略できます。
2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、ReceiverのConfigurationフォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、icaclient.admを選択します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. グループポリシーエディターで、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］の順に選択します。
7. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックして適切な設定を選択します。
   - ［TLS version］で［TLS v1.0］または［Detect version］を選択してTLSを有効にします。［Detect version］を選択した場合、ReceiverはTLS暗号化を使用して接続します。
   - ［SSL ciphersuite］で［Government］を選択します。
   - ［CRL verification］で［Require CRLs for connection］を選択します。

Web Interfaceを使用する場合は、SSL証明書をホストするサーバーのコンピューター名を指定します。 TLSを使ってReceiverとWeb Interfaceサーバー間の通信を保護する方法について詳しくは、Web Interfaceの情報を参照してください。

1. ［設定を変更］メニューの［サーバー設定］を選択します。
2. ［プラグインとこのサイト間の通信にSSL/TLSを使用する］チェックボックスをオンにします。
3. 変更を保存します。

SSL/TLSを有効にすると、すべてのURLでHTTPSプロトコルが使用されます。

接続時にTLSを使用するようにXenAppサーバーを構成して、Receiverとサーバー間の通信を保護することができます。

1. XenAppサーバー用のCitrix管理コンソールを開き、セキュリティを保護する公開アプリケーションの［アプリケーションプロパティ］ダイアログボックスを開きます。
2. ダイアログボックス左側のペインで［詳細設定］、［クライアントオプション］の順に選択し、［SSLおよびTLSを有効にする］チェックボックスをオンにします。
3. SSL/TLSプロトコルで保護するすべての公開アプリケーションで、このチェックボックスをオンにします。

Web Interfaceを使用する場合は、SSL証明書をホストするサーバーのコンピューター名を指定します。 TLSを使ってReceiverとWeb Interfaceサーバー間の通信を保護する方法について詳しくは、Web Interfaceの情報を参照してください。

TLSを使用するようにReceiverを構成して、ReceiverとWeb Interfaceサーバー間の通信を保護することができます。

有効なルート証明書がユーザーデバイスにインストールされていることを確認します。 詳しくは、「ユーザーデバイスへのルート証明書のインストール」を参照してください。

1. Windowsの通知領域でReceiverアイコンを右クリックし、［基本設定］を選択します。
2. ［プラグインの状態］の［Online Plug-in］のエントリを右クリックし、［サーバーの変更］を選択します。
3. ［サーバーの変更］ダイアログボックスに、現在構成されているURLが表示されます。 TLSを使って設定データを暗号化するには、サーバーURLを「https://<servername>」の形式で入力します。
4. ［更新］をクリックして変更を適用します。
5. ユーザーデバイス上のWebブラウザーでTLSを有効にします。 詳しい設定方法については、Webブラウザーのヘルプを参照してください。

ICAファイルに署名して信頼されていないサーバー上のアプリケーションやデスクトップが起動しないようにする

Feb 02, 2016

このトピックの内容は、管理用テンプレートを使用するWeb Interface環境にのみ適用されます。

ICAファイル署名機能は、認証していないアプリケーションやデスクトップをユーザーが起動しないようにするのに役立ちます。 信頼できるソースからアプリケーションを起動することをCitrix Receiverで検証し、管理ポリシーに基づいて信頼されていないサーバーからのアプリケーションまたはデスクトップの起動を防ぎます。 このアプリケーションまたはデスクトップの起動署名検証ためのReceiverセキュリティポリシーは、グループポリシーオブジェクト、Storefront、またはCitrix Merchandising Serverを使用して構成できます。 ICAファイル署名はデフォルトで無効になっています。 Storefrontに対するICAファイル署名については、Storefrontのドキュメントを参照してください。

Web Interface展開の場合、Web Interfaceでこの機能を有効にして構成し、Citrix ICA File Signing Serviceを使用して起動処理中にアプリケーションまたはデスクトップの起動に署名を含めることができます。 このサービスにより、コンピューターの個人証明書ストアにある証明書を使用してICAファイルに署名できます。

Citrix Merchandising ServerとReceiverを組み合わせて、起動署名検証を有効にして構成できます。これを行うには、Citrix Merchandising Server Administrator ConsoleのDeliveriesウィザードを使用して、信頼できる証明書の「拇印」を追加します。

グループポリシーオブジェクトを使用してアプリケーションまたはデスクトップの起動署名検証を有効にし設定するには、次の手順に従います。

1. 管理者として、［スタート］メニューからgpedit.mscを実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。
   注：既にica-file-signing.admテンプレートをグループポリシーオブジェクトエディターにインポートしている場合は、手順2.～5.は省略できます。
2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、ReceiverのConfigurationフォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、ica-file-signing.admを選択します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. グループポリシーエディターで、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］の順に選択し、［Enable ICA File Signing］を開きます。
7. ［有効］をクリックすると、信頼できる証明書のサムプリントのホワイトリストに署名証明書のサムプリントを追加したり、ホワイトリストから署名証明書のサムプリントを削除したりできます。これは、［表示］をクリックして［内容の表示］ダイアログボックスを使用して行います。 署名証明書のサムプリントは署名証明書のプロパティからコピーして貼り付けることができます。 ［Security Policy］ボックスの一覧から［Only allow signed launches（more secure）］または［Prompt user on unsigned launches（less secure）］を選択します。

オプション	説明
Only allow	正しく署名された、信頼できるサーバーからのアプリケーションまたはデスクトップの起動のみを

オプション	説明
signed launches（more secure）	許可します。 アプリケーションまたはデスクトップの起動に無効な署名がされている場合は、Receiverにセキュリティの警告メッセージが表示されます。 ユーザーは続行できず、承認されていない起動が禁止されます。
Prompt user on unsigned launches（less secure）	未署名または無効な署名のアプリケーションまたはデスクトップの起動が試行されるたびに、確認ダイアログボックスが開きます。 ユーザーはアプリケーションの起動を続行することも、起動を中止する（デフォルト）こともできます。

デジタル署名証明書を選択するときは、次の一覧の上位のオプションから順にお勧めします。

1. 周知の証明機関からコード署名証明書またはSSL署名証明書を購入する。
2. 社内に証明機関がある場合はその証明機関を使用して、コード署名証明書またはSSL署名証明書を作成する。
3. Web Interfaceのサーバー証明書などの既存のSSL証明書を使用する。
4. 新しいルート証明書を作成して、GPOまたは手動インストールによりユーザーデバイスに配布する。

シングルサインオンを有効にして信頼済みサーバーとの接続を保護するためのWebブラウザーとICAファイルの構成

Feb 02, 2016

このトピックの内容は、Web Interface環境にのみ適用されます。

シングルサインオンを使用したり、信頼済みサーバーへのセキュリティで保護された接続を管理したりするには、Citrixサーバーのサイトアドレスを Internet Explorerの［ローカルイントラネット］または［信頼済みサイト］ゾーンに追加します。これは、ユーザーデバイスのInternet Explorerで［ツール］、［インターネットオプション］、［セキュリティ］の順に選択して行います。 アドレスにはISM（Internet Security Manager）でサポートされるワイルドカード（*）を含めたり、「<protocol>://<URL>[:<port>]」のように具体的に指定する形式を使用したりできます。

ICAファイルとサイトゾーンのエントリの両方で同じ形式を使用する必要があります。 たとえば、ICAファイルで FQDN（Fully Qualified Domain Name：完全修飾ドメイン名）を使用した場合は、サイトゾーンのエントリでもFQDNを使用する必要があります。 XenDesktop接続ではデスクトップグループ名の形式のみを使用します。

http[s]://10.2.3.4

http[s]://10.2.3.*

http[s]://hostname

http[s]://fqdn.example.com

http[s]://*.example.com

http[s]://cname.*.example.com

http[s]://*.example.co.uk

desktop://group-20name

ica[s]://xaserver1

ica[s]://xaserver1.example.com

サイトゾーンにWeb Interfaceサイトの正確なアドレスを追加します。

Webサイトのアドレスの例

https://my.company.com

http://10.20.30.40

http://server-hostname:8080

https://SSL-relay:444

アドレスは「<desktop>//<Desktop Group Name>」の形式で追加します。 デスクトップグループ名（）にスペースが含まれる場合、各スペースを「-20」で置き換えます。

ICAファイルでは、Citrixサーバーのサイトアドレスを次の形式で指定します。 このアドレスを同じ形式で、Internet Explorerの［ローカルイントラネット］または［信頼済みサイト］ゾーンに追加します。これは、ユーザーデバイスのInternet Explorerで［ツール］、［インターネットオプション］、［セキュリティ］の順に選択して行います。

ICAファイルのHttpBrowserAddressエントリの例

HttpBrowserAddress=XMLBroker.XenappServer.example.com:8080

ICAファイルのXenAppサーバーアドレスエントリの例

ICAファイルにXenAppサーバーの**Address**フィールドのみが含まれる場合、次の形式のいずれかを使用します。

icas://10.20.30.40:1494

icas://my.xenapp-server.company.com

ica://10.20.30.40

クライアントリソースのアクセス許可を設定するには

Mar 14, 2016

このトピックの内容は、Web Interface環境にのみ適用されます。

信頼済みサイトおよび制限付きサイトのゾーンを使用して、次の方法でクライアントリソースのアクセス許可を設定できます。

- 信頼済みサイトにWeb Interfaceのサイトを追加する
- 新しいレジストリ設定を変更する

> ## 注意
>
> Citrix Receiverの最近の機能拡張のより、以前のバージョンのプラグイン/Receiverで使用できたINIファイルによる手順は、次の手順により置き換えられました。

> ## 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。 レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。 レジストリエディターは、お客様の責任と判断の範囲でご使用ください。 また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. Internet Explorerの［ツール］メニューで［インターネットオプション］>［セキュリティ］の順に選択します。
2. ［信頼済みサイト］アイコンをクリックし、［サイト］をクリックします。
3. ［このWebサイトをゾーンに追加する］ボックスにWeb InterfaceのサイトのURLを入力して［追加］をクリックします。
4. http://support.citrix.com/article/CTX133565からレジストリ設定をダウンロードしてレジストリを変更します。32ビット版WindowsのユーザーデバイスにはSsonRegUpx86.regを、64ビット版WindowsのユーザーデバイスにはSsonRegUpx64.regを使用します。
5. ユーザーデバイスからログオフしてログオンします。

1. http://support.citrix.com/article/CTX133565からレジストリ設定をダウンロードして各ユーザーデバイスに設定をインポートします。 32ビット版WindowsのユーザーデバイスにはSsonRegUpx86.regを、64ビット版WindowsのユーザーデバイスにはSsonRegUpx64.regを使用します。
2. レジストリエディターを開いてHKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Client Selective Trustに移動し、次のリソースのデフォルト値を適切なゾーンにおいて必要なアクセス値に変更します。

リソースキー	リソースの説明
FileSecurityPermission	クライアント側ドライブ
MicrophoneAndWebcamSecurityPermission	マイクおよびWebカメラ

リソースキー ScannerAndDigitalCameraSecurityPermission	リソースの説明 USBおよびそのほかのデバイス

値	説明
0	アクセスなし
1	読み取り専用アクセス
2	フルアクセス
3	アクセスするかどうかユーザーに確認

Citrix Receiverがアプリケーションを列挙していてStorefrontと通信している場合、Windowsプラットフォーム暗号化が使用されます。

Citrix ReceiverとXenApp/XenDesktop間のTCP接続の場合、Citrix Receiverは次の暗号の組み合わせともにTLS 1.0、1.1、および1.2をサポートします。

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

UDPベースの接続の場合、Citrix Receiverは次の暗号の組み合わせと共にDTLS 1.0をサポートします。

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

SP 800-52準拠モードの有効化

［コンピューターの構成］>［管理テンプレート］>［Citrix Components］>［Network Routing］>［TLS and Compliance Mode Configuration］の下に、**[Enable FIPS]**というチェックボックスが実装されました。 このチェックボックスをオンにすると、すべてのICAコネクションに対してFIPS準拠の暗号化のみが使用されます。 デフォルトでは、このオプションは無効になっています。

新しいセキュリティ準拠モードであるSP 800-52が実装されています。 デフォルトでは、このオプションは無効になっています。 NIST SP 800-52で必要なコンプライアンスについて説明した次のリンクを参照してください。http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295

> **注意**
>
> SP800-52準拠モードはFIPSコンプライアンスを必要とします。 SP800-52が有効な場合、FIPS設定とは関係なくFIPSモードも有効になります。 Certificate Revocation Checkポリシーの値は［Full access check and CRL required］または［Full access check and CRL required All］に設定します。

TLSバージョンと暗号の組み合わせの制限

Citrix Receiverを構成してTLSバージョンと暗号化の組み合わせを制限できます。 ICAコネクションのTLSプロトコルを決定するための、許可されたTLSプロトコルのバージョンを選択するオプションがあります。 クライアントとサーバー間で相互に使用できる最新のTLSバージョンが選択されます。 次のオプションがあります。

- TLS 1.0 | TLS 1.1 | TLS 1.2（デフォルト）
- TLS 1.1 | TLS 1.2
- TLS 1.2

このオプションはAndroid 3.0以降で使用できます。 Citrix Receiverは次のものを選択できます。

- 任意
- Commercial
- Government

商用暗号の組み合わせ

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

公用商用暗号の組み合わせ

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **注意**
>
> **［Require TLS for all connections］**が有効な場合、StoreFrontへの接続要求にもHTTPSが必要です。HTTPとしてのストアの追加に失敗し、非SSL VDA（XenDesktopおよびXenApp）を起動できません。

Receiver Desktop Lock

Aug 30, 2016

ユーザーがローカルのデスクトップを操作する必要がない場合は、Receiver Desktop Lockを使用できます。 ユーザーはDesktop Viewer（有効な場合）を引き続き使用することはできますが、ツールバー上には必須オプションセットであるCtrl+Alt+Del、基本設定、デバイス、および切断しかありません。

Citrix Receiver Desktop Lockはドメイン参加のマシンで機能し、SSON対応（シングルサインオン）でストアが構成されています。またこれは、SSONが有効ではない非ドメイン参加のマシンでも使用できます。 Program Neighborhoodエージェントサイトはサポートしません。 以前のバージョンのDesktop Lockは、Receiver for Windows 4.2.xへアップグレードするとサポートされません。

Citrix Receiver for Windowsを /includeSSON フラグを使ってインストールする必要があります。 adm/admxファイルまたはコマンドレットオプションのいずれかを使って、ストアおよびシングルサインオンを構成する必要があります。 詳しくは、「コマンドインを使ったCitrix Receiverのインストールと構成」を参照してください。

次に、管理者としてcitrix.com/downloadsにあるCitrixReceiverDesktopLock.MSIを使ってReceiver Desktop Lockをインストールします。

Citrix Receiver Desktop Lockのシステム要件

- Windows 7（Embedded Editionを含む）、Windows 7 Thin PC、Windows 8、およびWindows 8.1でサポートされます。
- ユーザーデバイスをローカルエリアネットワーク（LAN）またはワイドエリアネットワーク（WAN）に接続する必要があります。

ローカルアプリケーションアクセス

> **Important**
>
> ローカルアプリケーションアクセスを有効にすると、グループポリシーオブジェクトテンプレートまたは同様のポリシーでフルロックダウンが適用されていない限り、ローカルデスクトップアクセスを実行できます。 詳しくは、XenAppおよびXenDesktopのドキュメントで「ローカルアプリケーションアクセスとURLリダイレクトの構成 を参照してください。

Receiver Desktop Lockの実行

- Receiver Desktop Lockを使って次のReceiver for Windowsの機能を実行できます。
  - 3Dpro、Flash、USB、HDX Insight、Microsoft Lync 2013プラグイン、およびローカルアプリケーションアクセス
  - ドメイン、2要素、またはスマートカード認証のみ
- Receiver Desktop Lockセッションを切断するとエンドデバイスをログアウトします。
- FlashのリダイレクトはWindows 8以降では無効です。 Windows 7では有効です。
- Desktop ViewerはHome、Restore、Maximize、およびDisplayプロパティがないReceiver Desktop Lockに最適化されています。
- Viewerのツールバーでは、Ctrl+Alt+Delキーの組み合わせを使用できます。
- Windows+Lキー以外のほとんどのWindowsショートカットキーをリモートセッションで実行できます。 詳しくは、「リモートセッションでのWindowsショートカットキーの実行」を参照してください。
- 接続を無効にするまたはデスクトップ接続のDesktop Viewerを無効にする場合、Ctrl+F1キーを押すとCtrl+Alt+Delを押すのと同じように動作します。

Receiver Desktop Lockをインストールするには

この手順に従ってReceiver for Windowsをインストールすると、Receiver Desktop Lockで仮想デスクトップが表示されます。 ス

マートカードを使用する展開については、「Receiver Desktop Lockを実行するデバイスでスマートカードを使用できるように構成するには」を参照してください。

1. ローカルの管理者アカウントを使用してログオンします。
2. コマンドプロンプトで次のコマンド（インストールメディアのCitrix Receiver and Plug-ins > Windows > Receiverフォルダーにあります）を実行します。
   次に例を示します。
   CitrixReceiver.exe /includeSSON STORE0="*DesktopStore*;https://*my.storefront.server*/Citrix/MyStore/discovery;on;*Desktop Store*"
   コマンドの詳細については、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」でReceiver for Windowsのインストールに関する説明を参照してください。
3. インストールメディアの同じフォルダーにあるCitrixReceiverDesktopLock.MSIをダブルクリックします。 Desktop Lockウィザードが開きます。 画面の指示に従って操作します。
4. インストールが完了したら、ユーザーデバイスを再起動します。 デスクトップへのアクセスが許可されていて、ドメインユーザーとしてログオンすると、Receiver Desktop Lockでデスクトップが表示されます。

ただし、インストールの完了後にユーザーデバイスを管理できるようにするため、CitrixReceiverDesktopLock.msiをインストールしたときのアカウントでは代替シェルが使用されません。 このアカウントを削除すると、デバイスにログオンして管理することができなくなります。

Receiver Desktop Lockの**サイレントインストール**を実行するには、次のコマンドラインを使用します。msiexec /i CitrixReceiverDesktopLock.msi /qn

Receiver Desktop Lockを構成するには

Receiver Desktop Lockを使用するユーザーには、単一の仮想デスクトップだけのアクセスを付与します。

Active Directoryポリシーを使用して、ユーザーが仮想デスクトップを休止状態にできないようにします。

Receiver Desktop Lockを構成するときは、インストール時に使用した管理者アカウントを使用します。

- Receiver.admx（またはReceiver.adml）とReceiver_usb.admx（.adml）ファイルがグループポリシーにロードされていることを確認します（ポリシーは［コンピューターの構成］または［ユーザーの構成］>［管理用テンプレート］>［従来の管理用テンプレート（ADMX）］>［Citrix Components］の順に展開すると表示されます）。 これらの.admxファイルは、%Program Files%\Citrix\ICA Client\Configuration\にインストールされています。
- USB基本設定 — ユーザーがUSBデバイスを接続すると、そのデバイスは自動的に仮想デスクトップで使用可能になります。このとき、ユーザーが何らかの操作を行う必要はありません。 USBドライブの制御と表示は、仮想デスクトップにより処理されます。
  - USBポリシー規則を有効にします。
  - ［Citrix Receiver］>［Remoting client devices］>［Generic USB Remoting］の順に選択して、Existing USB DevicesとNew USB Devicesポリシーを有効にして構成します。
- ドライブマッピング — ［Citrix Receiver］、［Remoting client devices］の順に選択して、［Client drive mapping］ポリシーを有効にして構成します。
- マイク — ［Citrix Receiver］、［Remoting client devices］の順に選択して、［Client microphone］ポリシーを有効にして構成します。

Receiver Desktop Lockを実行するデバイスでスマートカードを使用できるように構成するには

1. StoreFrontを構成します。
   1. Citrix XML ServiceのDNSアドレス解決を有効にして、Kerberos認証を使用できるように構成します。
   2. StoreFrontサイトのHTTPSアクセスを構成して、ドメインの証明機関による署名付きのサーバー証明書を作成し、デフォルトのWebサイトにHTTPSバインドを追加します。
   3. ［スマートカードパススルー認証］が有効になっていることを確認します（デフォルトで有効になっています）。
   4. ［Kerberos］を有効にします。

5. ［Kerberos］および［スマートカードパススルー認証］を有効にします。
6. IISのDefault Web Siteで［匿名アクセス］を有効にして、［統合Windows認証］を使用します。
7. IISのDefault Web SiteのSSL設定で［SSLが必要］チェックボックスがオフで、［クライアント証明書］で［無視］が選択されていることを確認します。

2. グループポリシー管理コンソールを使用して、ユーザーデバイスでローカルコンピューターのポリシーを構成します。
   1. %Program Files%\Citrix\ICA Client\Configuration\からReceiver.admxテンプレートをインポートします。
   2. ［管理用テンプレート］>［従来の管理用テンプレート（ADMX）］>［Citrix Components］>［Citrix Receiver］>［User authentication］の順に展開します。
   3. ［Smart card authentication］を有効にします。
   4. ［Local user name and password］を有効にします。
3. Receiver Desktop Lockをインストールする前に、ユーザーデバイスを構成します。
   1. Windows Internet Explorerの信頼済みサイトの一覧に、Delivery ControllerのURLを追加します。
   2. Windows Internet Explorerの信頼済みサイトの一覧に、最初のデリバリーグループのURLを「desktop://<デリバリーグループ名>」形式で追加します。
   3. 信頼済みサイトに対するInternet Explorerの自動ログオン機能を有効にします。

Receiver Desktop Lockがユーザーデバイスにインストールされている場合、スマートカード取り出し時の動作に競合が生じないようにポリシーが適用されます。 たとえば、スマートカード取り出し時の動作がデスクトップ側で［ログオフを強制する］に設定されている場合、ユーザーデバイスのWindows側の設定にかかわらず、ユーザーデバイスからも強制的にログオフされます。 これにより、ユーザーデバイスの整合性が維持されます。 これは、Receiver Desktop Lockがあるユーザーデバイスにのみ適用されます。

Receiver Desktop Lockをアンインストールするには

以下のコンポーネントを両方ともアンインストールする必要があります。

1. Recevier Desktop Lockのインストールと構成に使用したローカル管理者アカウントでログオンします。
2. プログラムの削除や変更を行うためのWindows機能（コントロールパネルの［プログラムと機能］など）を開き、以下の操作を行います。
   - ［Citrix Receiver Desktop Lock］をアンインストールします。
   - Citrix Receiverをアンインストールします。

リモートセッションでのWindowsショートカットキーの実行

ほとんどのWindowsショートカットキーはリモートセッションで実行できます。 このセクションでは、一般的なものについていくつか説明します。

Windows

- Win+D - すべてのウィンドウをデスクトップ上で最小化します。
- Alt+Tab - アクティブなウィンドウを変更します。
- Ctrl+Alt+Delete - Ctrl+F1およびDesktop Viewerツールバーを介します。
- Alt+Shift+Tab
- Windows+Tab
- Windows+Shift+Tab
- Windows+すべての文字キー

Windows 8

- Win+C - チャームを開きます。
- Win+Q - チャームを検索します。
- Win+H - チャームを共有します。
- Win+K - デバイスのチャーム。
- Win+I - 設定のチャーム。
- Win+Q - アプリを検索します。
- Win+W - 設定を検索します。

- Win+F - ファイルを検索します。

Windows 8のアプリ

- Win+Z - アプリのオプションを開きます。
- Win+. - アプリを左にスナップします。
- Win+Shift+. - アプリを右にスナップします。
- Ctrl+Tab - アプリ履歴を循環させます。
- Alt+F4 - アプリを閉じます。

Desktop

- Win+D - デスクトップを開きます。
- Win+, - デスクトップでプレビューします。
- Win+B - デスクトップに戻ります。

Other

- Win+U - コンピューターの簡単操作センターを開きます。
- Ctrl+Esc - 画面を開始します。
- Win+Enter - Windowsナレーターを開きます。
- Win+X - システムユーティリティ設定メニューを開きます。
- Win+PrintScrn - スクリーンショットを取りピクチャに保存します。
- Win+Tab - スイッチ一覧を開きます。
- Win+T - タスクバーの開いているウィンドをプレビューします。